

# Low rank matrix recovery from Clifford orbits

Richard Kueng,<sup>1</sup> Huangjun Zhu,<sup>1</sup> and David Gross<sup>1,2</sup>

<sup>1</sup>*Institute for Theoretical Physics, University of Cologne, Germany*

<sup>2</sup>*Centre for Engineered Quantum Systems, School of Physics,  
The University of Sydney, Sydney, NSW 2006, Australia*

(Dated: October 27, 2016)

We prove that low-rank matrices can be recovered efficiently from a small number of measurements that are sampled from orbits of a certain matrix group. As a special case, our theory makes statements about the *phase retrieval* problem. Here, the task is to recover a vector given only the *amplitudes* of its inner product with a small number of vectors from an orbit. Variants of the group in question have appeared under different names in many areas of mathematics. In coding theory and quantum information, it is the *complex Clifford group*; in time-frequency analysis the *oscillator group*; and in mathematical physics the *metaplectic group*. It affords one particularly small and highly structured orbit that includes and generalizes the discrete Fourier basis: While the Fourier vectors have coefficients of constant modulus and phases that depend linearly on their index, the vectors in said orbit have phases with a quadratic dependence. In quantum information, the orbit is used extensively and is known as the set of *stabilizer states*. We argue that due to their rich geometric structure and their near-optimal recovery properties, stabilizer states form an ideal model for structured measurements for phase retrieval. Our results hold for  $m \geq C\kappa_r d \log(d)$  measurements, where the oversampling factor  $\kappa_r$  varies between  $\kappa_r = 1$  and  $\kappa_r = r^2$  depending on the orbit. The reconstruction is stable towards both additive noise and deviations from the assumption of low rank. If the matrices of interest are in addition positive semidefinite, reconstruction may be performed by a simple constrained least squares regression. Our proof methods could be adapted to cover orbits of other groups.

## I. MOTIVATION

### A. Phase retrieval

Starting point of this paper is the *phase retrieval problem* [1]. The problem is to reconstruct an unknown vector  $x \in \mathbb{C}^d$  from measurements of the form

$$y_k = |\langle a_k, x \rangle|^2 + \epsilon_k \quad 1 \leq k \leq m. \quad (1)$$

Here, the  $a_1, \dots, a_m \in \mathbb{C}^d$  model linear measurements and the  $\epsilon_k$ 's additive noise. The phase retrieval problem occurs in many areas of science, for example in X-ray crystallography [2], astronomy [3, 4] and diffraction imaging [5, 6], as well as pure state quantum estimation theory [7–11].

While a number of (often heuristic) algorithms for solving the inverse problem (1) have long been used [12], a rigorous analysis is quite involved. Even in the absence of noise ( $\epsilon_k = 0$ ), it is not obvious how many measurements are necessary, which measurements can be employed, and whether the vector  $x$  can be recovered in a numerically stable and computationally efficient way.

Recently, techniques from convex optimization theory have been used with great success to analyze the phase retrieval problem. This ansatz is known as *PhaseLift* [13, 14]. Beyond suggesting an algorithm for reconstruction, it brings powerful methods—e.g. convex duality theory—into the fold. There is now a fast-growing body of literature (including [15–25]) using these tools to establish recovery guarantees for phase retrieval for a variety of measurement models.

The present paper is also based on PhaseLift, and we will review the technique in Section III below. However, our main focus lies on identifying a new class of measurement vectors  $a_1, \dots, a_m$  for which the phase retrieval problem can be proven to be well-posed. Consequently, we start the introduction by discussing these measurement models.

### B. Measurement models

While some deterministic sets of measurements vectors for the phase retrieval problem have recently been described [11, 26–28], most constructions are randomized. The typical result states that if the  $m$  vectors  $a_k$  are drawn independently according to some distribution in  $\mathbb{C}^d$ , the inverse problem associated with (1) is well-posed with overwhelming probability. An incomplete and *ad hoc* classification of known examples might look as follows:

*Gaussian or Haar distributions.*—The strongest, easiest to prove, and earliest examples used Gaussian random vectors, or vectors drawn uniformly from the unit-sphere (*Haar* distribution) [14, 15]. While powerful, this ensemble is rarely suitable in practical applications and gives no indication as to which particular properties are necessary for phase retrieval. These two deficits are addressed by the next two categories.

*Ensembles modeled after particular applications.*—Measurements modeling practical applications have been analyzed. An early example is given by the works on *coded diffraction patterns* that are motivated by problems arising in diffraction imaging [18, 19]. While

highly relevant, the arguments tend to be very specific to the particular use case.

*Designs.*—In contrast, one can ask for weak abstract properties of ensembles that are sufficient for phase retrieval. Since the proofs establishing recovery guarantees typically require information on higher moments  $\mathbb{E}[a^{\otimes t}(a^*)^{\otimes t}]$  of the random measurement vectors, Ref. [16] analyzed the suitability of *complex projective  $t$ -designs* [29, 30] for phase retrieval, see also [31, 32]. These are ensembles that reproduce the first  $2t$ -th moments of the uniform distribution on the sphere. This program has been successful in the sense that excellent recovery guarantees for designs of degree  $t \geq 4$  have been established [21]. At the same time, it has not yet lived up to some early expectations, because constructions known for infinite families of 4-designs [33, 34] are arguably significantly less explicit and “well-structured” as is the case for  $t = 3$  [35–37], or lower [38, 39]. Amending this situation was one of the motivations for the present work.

Here, we pursue a different route and establish representation-theoretic techniques for deriving recovery guarantees for measurement vectors sampled uniformly from orbits of matrix groups. We pay particular attention to the *complex Clifford group* and its orbit of *stabilizer states*, introduced below.

Stabilizer states have appeared in several areas of science. They are particularly central to quantum information theory. Therefore, this (and closely related [40]) results might find direct practical applications e.g. in quantum state estimation [41, 42].

Beyond that, however, we want to put forth the argument that stabilizer states provide an ideal model for phase retrieval measurements, due to their rich geometric structure and the near-optimal recovery guarantees that can be proved.

The remaining paragraphs of this section are somewhat subjective and speculative. Readers more interested in mathematical meat than meta-mathematical chatter should skip ahead.

To explain what we have in mind, we recall the situation for related inverse problems that can be tackled using convex optimization theory [43]: *compressed sensing* for sparse vectors, and *low-rank matrix recovery*.

Also in compressed sensing, first results pertained to Gaussian measurements [43–45]. Attention then quickly shifted to “more structured” models, with the most natural one being measurements sampled from the Fourier basis [46, 47]. Beyond its practical relevance, the high degree of a geometric and algebraic structure connected to Fourier vectors makes their study particularly fruitful. The absolutely tight bounds in [48] serve as one example.

The story is similar in low-rank matrix recovery. Initial results are for Gaussian measurements [49], with follow-up work concentrating on the practically relevant measurement model of random matrix elements [50–52]. A measurement model whose “high degree of

structure” allows for a particularly simple analysis is given by the *Pauli basis* [53–56]. For example, the fact that it constitutes a *unitary operator basis* yields short proofs and tight bounds on the sampling rate. What is more, its rich algebraic structure has been a crucial ingredient to a matching converse bound [54, Theorem 15].

Arguably, a measurement model for phase retrieval, that would take up a role analogous to the ones plaid by the Fourier and Pauli bases, has not yet emerged. A main reason may be the lack of obvious candidates: There are just not that many infinite families of high-dimensional vector configurations that have been widely studied. To the present authors, the set of stabilizer states constitutes a worthy candidate for that role.

## II. STABILIZER STATES AND THE CLIFFORD GROUP

Here, we introduce the concepts of *stabilizer states* and the (complex) *Clifford group* from various points of view. These, and related notions, have been discovered several times in different branches of science and mathematics, including quantum information theory [57], coding theory [58, 59], time-frequency analysis [60, 61], as well as mathematical physics and functional analysis [62–64].

Owing to the upbringing of the authors, we initially adopt the vantage point of quantum information, where these concepts go back to Ref. [57]. The textbook [65] treats them extensively. A point of view focused on connections to symplectic geometry is given in Refs. [37, 66]. Here, we mainly summarize results from these sources.

In Section II E, we comment on related groups and give some pointers to the literature of other fields (though we are by no means experts in this regard).

### A. Stabilizer states: Elementary approach

In this section, we provide a concrete basis representation of stabilizer states. While very transparent, it turns out that calculations are best done using an indirect representation in terms of *stabilizer groups* or certain structures from symplectic geometry. This point of view is described in the following sections.

We first recall the definition of the Fourier basis associated with the discrete vector space  $\mathbb{Z}_2^n$ . To this end, we label the standard basis  $\{e_x\}_x$  of  $\mathbb{C}^{2^n}$  by vectors  $x \in \mathbb{Z}_2^n$ . A *Fourier vector*  $f_l \in \mathbb{C}^{2^n}$  depends on a  $\mathbb{Z}_2$ -linear form  $l : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$  and has expansion coefficients given by

$$(f_l)_x = 2^{-n/2} (-1)^{l(x)}. \quad (2)$$

Essentially, stabilizer states are obtained by generalizing (2) to allow for a *quadratic* dependence of the phase on the label  $x$ . Indeed, the simplest type of stabilizer

state  $\psi_q$  is defined by a *quadratic form*  $q$  on  $\mathbb{Z}_2^n$  and has expansion coefficients

$$(\psi_q)_x = 2^{-n/2} (-1)^{q(x)}. \quad (3)$$

The most general form goes beyond Eq. (3) in two ways: (i) The non-zero coefficients can be restricted to an affine subset of  $\mathbb{Z}_2^n$ , and (ii) certain complex phase factors are also allowed. To be precise [67, 68]:

**Definition 1.** A stabilizer state  $\psi \in \mathbb{C}^{2^n}$  is defined by the following data:

1. An affine subset  $A \subset \mathbb{Z}_2^n$ ,
2. a quadratic form  $q : A \rightarrow \mathbb{Z}_2$ ,
3. a linear form  $l : A \rightarrow \mathbb{Z}_2$ .

Its components are

$$\psi_x = \begin{cases} |A|^{-1/2} i^{l(x)} (-1)^{q(x)} & x \in A \\ 0 & x \notin A. \end{cases}$$

More explicitly, recall that the standard inner product gives rise to a one-one correspondence between linear forms  $l_y$  on  $\mathbb{Z}_2^n$  and elements  $y$  of  $\mathbb{Z}_2^n$  via

$$l_y(x) := \langle y, x \rangle = \sum_{i=1}^n y_i x_i \pmod{2}.$$

A quadratic form  $q$  on  $\mathbb{Z}_2^n$  is a function that can be written as

$$q(x) = \sum_{i \leq j} q_{i,j} x_i x_j \pmod{2}, \quad (4)$$

for some upper triangular matrix  $q_{i,j}$ . Because in characteristic 2, it holds that  $x_i^2 = x_i$ , Eq. (4) includes linear forms as a special case:

$$\langle x, y \rangle = \sum_{i \leq j} \text{diag}(y)_{i,j} x_i x_j,$$

where  $\text{diag}(y)$  is the matrix with the vector  $y$  on its main diagonal. In particular, the Fourier basis is included in the set of stabilizer states.

Many properties of stabilizer states are known. E.g. they can be partitioned into disjoint sets of ortho-normal bases; and the inner product between two stabilizer states depends essentially only on the basis they belong to. All these properties are hard to see from their basis expansion. The formalism of *stabilizer groups*, introduced next, is less explicit, but makes such computations much easier.

## B. Stabilizer states from stabilizer groups

Stabilizer states can be defined implicitly as the common eigenvectors of maximal sets of commuting Pauli operators.

To make this precise, define the *Pauli operators* on  $\mathbb{C}^2$  as

$$\begin{aligned} \sigma_{(0,0)} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & \sigma_{(0,1)} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \\ \sigma_{(1,0)} &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, & \sigma_{(1,1)} &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \end{aligned} \quad (5)$$

A Pauli operator  $W_a$  on

$$\underbrace{\mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2}_{n \text{ factors}} \simeq \mathbb{C}^{2^n}$$

is defined as the tensor product of  $n$  such matrices:

$$W_a := \sigma_{(a_1, a_2)} \otimes \dots \otimes \sigma_{(a_{2n-1}, a_{2n})}. \quad (6)$$

Clearly, the index  $a$  takes values in the  $\mathbb{Z}_2$ -vector space  $\mathbb{Z}_2^{2n}$ .

We denote the set of all Pauli operators on  $\mathbb{C}^{2^n}$  by

$$\bar{\mathcal{P}}_n = \{W_a \mid a \in \mathbb{Z}_2^{2n}\}.$$

The *Pauli group*  $\mathcal{P}_n$  is the group generated by all the Pauli operators in  $\bar{\mathcal{P}}_n$ . It turns out that the group consists of the Pauli operators multiplied by phase factors that are powers of the imaginary unit  $i$ :

$$\mathcal{P}_n = \langle \bar{\mathcal{P}}_n \rangle = \{i^j W_a \mid a \in \mathbb{Z}_2^{2n}, j \in \mathbb{Z}_4\}.$$

**Definition 2.** A stabilizer group is a subgroup  $S \subset \mathcal{P}_n$  of the Pauli group such that

1.  $S$  is abelian,
2.  $S$  does not contain  $-\mathbb{1}$ ,
3.  $S$  has cardinality<sup>1</sup>  $|S| = 2^n$ .

Because a stabilizer group  $S$  is abelian, there is an eigenbasis common to all  $W \in S$ . It turns out that this basis is unique (up to phase factors) and given by stabilizer states. Every stabilizer state arises this way.

In fact, it suffices to consider the joint  $(+1)$ -eigenspace:

**Proposition 1.** There is a one-one correspondence between stabilizer states and stabilizer groups.

Given a stabilizer state  $\psi \in \mathbb{C}^{2^n}$ , the associated stabilizer group is

$$S = \{W \in \mathcal{P}_n \mid W\psi = \psi\}.$$

Given a stabilizer group  $S \subset \mathcal{P}_n$ , a projection onto the associated stabilizer state is

$$\psi\psi^* = 2^{-n} \sum_{W \in S} W.$$

<sup>1</sup> There is a theory that generalizes stabilizer states to so-called *stabilizer codes* [57, 65] and, for that purpose, drops the restriction on the cardinality of  $S$ . However, we do not require these concepts in the present paper and thus stick to the more restrictive definition.

In quantum information theory, stabilizer states are usually introduced this way, and not using the basis representation we gave in the previous section. This explains the name.

### C. The symplectic connection

There is a more abstract way to look at stabilizer states in terms of certain objects in discrete symplectic vector spaces (c.f. e.g. [37, 66] and references therein). We will briefly introduce this connection next.

Symplectic structures appear in the composition law and the commutation relation of Pauli operators. To explain this, let  $J$  be the  $2n \times 2n$  block-diagonal matrix with  $n$  blocks of  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  on the diagonal. Then

$$[a, b] = a^T J b$$

defines a *symplectic form* on  $\mathbb{Z}_2^{2n}$ . One can then verify that the commutation relation

$$W_a W_b = (-1)^{[a, b]} W_b W_a \quad (7)$$

holds. With a slight abuse of notation, the group law of the Pauli group can be written as

$$W_a W_b = i^{[a, b]} W_{a+b}, \quad (8)$$

where the arithmetic in the exponent of  $i$  is to be performed modulo 4 (as opposed to in  $\mathbb{Z}_2$ ).

We can use these relations to analyze the structure of stabilizer groups. Let  $S \subset \mathcal{P}_n$  be a stabilizer group. It is of the form

$$S = \{(-1)^{s(a)} W_a \mid a \in M\} \quad (9)$$

for some set  $M \subset \mathbb{Z}_2^{2n}$  and some function  $s : M \rightarrow \mathbb{Z}_2$ . Pauli operators with complex coefficients  $\pm i W_a$  cannot occur inside a stabilizer group, for else their square

$$(\pm i W_a)^2 = -\mathbb{1}$$

would also be an element of the group, contrary to Definition 2.

Because  $S$  is a group and because (8) states that composition of Pauli operators  $W_a W_b$  corresponds to addition  $a + b$  of their indices, it follows that  $M$  is closed under addition and hence a subspace of  $\mathbb{Z}_2^{2n}$ . The fact that  $S$  is abelian and the commutation relation (7) together imply that the symplectic form  $[\cdot, \cdot]$  vanishes on  $M$ . Such spaces are called *isotropic* in symplectic geometry. Finally, the fact that  $|S| = 2^n$  means that  $M$  has dimension  $n$  as a subspace of  $\mathbb{Z}_2^{2n}$ . As isotropic subspaces can have at most half the dimension of the ambient vector space, this means that  $M$  is a *maximal isotropic subspace*, or a *Lagrangian subspace*.

Next, we turn to the phase function  $s : M \rightarrow \mathbb{Z}_2$  defined in (9). Its value can be chosen freely on a basis

$\{b_1, \dots, b_n\}$  of  $M$ . This choice gives rise to a generating set

$$S = \{(-1)^{s(b_1)} W_{b_1}, \dots, (-1)^{s(b_n)} W_{b_n}\},$$

which extends  $s$  uniquely to all of  $M$ . In this way, one obtains  $2^n$  different stabilizer groups for any given  $M$  and one can show that this set does not depend on the choice of basis for  $M$ .

The  $2^n = d$  stabilizer states associated to any given Lagrangian subspace  $M$  turn out to form an orthonormal basis for  $\mathbb{C}^d$ . Thus, the set of stabilizer states can be partitioned into disjoint orthonormal bases.

To summarize:

**Proposition 2.** *A stabilizer group  $S \subset \mathcal{P}_n$  can be specified by the following data:*

1. *A Lagrangian subspace  $M \subset \mathbb{Z}_2^{2n}$ ,*
2. *a phase function  $s : M \rightarrow \mathbb{Z}_2$ , which can be freely chosen on a basis  $\{b_1, \dots, b_n\}$  of  $M$ .*

*The stabilizer group  $S$  is then generated by the  $n$  Pauli operators  $(-1)^{s(b_k)} W_{b_k}$  for  $k = 1, \dots, n$ .*

### D. Symmetries: The Clifford group

Most important for our analysis below is the fact that the set of stabilizer states affords a large, transitive symmetry group. To introduce it, we define the *Clifford group* as follows<sup>2</sup>.

**Definition 3.** *The Clifford group  $\text{Cl}_n$  is the normalizer of  $\mathcal{P}_n$  inside of  $U(2^n)$ .*

In other words,  $\text{Cl}_n$  is the set of unitaries  $U$  such that, for all Pauli operators  $W_a$ , it holds that

$$U W_a U^\dagger \in \mathcal{P}_n.$$

Because the Clifford group maps elements of the Pauli group to elements of the Pauli group under conjugation, it also maps stabilizer groups to stabilizer groups. By the

<sup>2</sup> We remark that the term *Clifford group* sometimes refers to a minor variant of the group introduced here. Indeed, note that if  $U \in \text{Cl}_n$ , then so is  $e^{i\phi} U$  for every phase  $\phi$ . For our purposes, these phase factors are unimportant. But often, it is desirable to work with a version of the Clifford group that includes as few phases as possible in the sense that its intersection with the center  $Z = \{e^{i\phi} \mathbb{1}\}_{\phi \in \mathbb{R}}$  of  $U(2^n)$  is the smallest. One can find explicit generators for a group  $\text{Cl}'_n$  which is identical to  $\text{Cl}_n$  up to phases in that  $\text{Cl}'_n / Z = \text{Cl}_n / Z$  and such that  $\text{Cl}'_n \cap Z = \{i, -1, 1, -i\}$ , which is minimal [69]. We also remark that the term *Clifford group* is sometimes used to refer to the cover group of the orthogonal group that is given by the invertible elements inside a *Clifford algebra*. Despite this unfortunate coincidence in names, there seems to be no connection between this group and the one used here.



preceding sections, this means that the Clifford group maps stabilizer states onto stabilizer states. That action is known to be transitive—i.e. the set of stabilizer states forms an orbit under the Clifford group.

From Equation (7), it follows that for any pair of Pauli operators  $W_a, W_b$  it holds that

$$W_a W_b W_a^\dagger = \pm W_b.$$

Thus the Pauli group forms a subgroup of the Clifford group  $\mathcal{P}_n \subset \text{Cl}_n$ .

More interesting is the quotient of the Clifford group up to phases and the Pauli group. To explain it, note that since an action by conjugation preserves group laws and since the group law (8) of the Pauli group is tied to both the linear structure and the symplectic form on  $\mathbb{Z}_2^{2n}$ , it seems plausible that discrete symplectic groups might play a role. This is indeed true. Let  $\text{Sp}(2n, \mathbb{Z}_2)$  be the *symplectic group* composed of all  $2n \times 2n$  matrices  $F$  over  $\mathbb{Z}_2$  that satisfy the relation

$$FJF^T = J. \quad (10)$$

Then we have:

**Proposition 3.** *For every  $U \in \text{Cl}_n$ , there is a unique symplectic matrix  $F \in \text{Sp}(2n, \mathbb{Z}_2)$  such that*

$$UW_aU^\dagger = (-1)^{f(a)}W_{Fa} \quad \forall a \in \mathbb{Z}_2^{2n}, \quad (11)$$

where  $f$  is a function from  $\mathbb{Z}_2^{2n}$  to  $\mathbb{Z}_2$ . Conversely, for each symplectic matrix  $F \in \text{Sp}(2n, \mathbb{Z}_2)$  there exists a  $U \in \text{Cl}_n$  and a suitable function  $f$  such that the above equation is satisfied.

Note that Clifford unitaries of the form  $e^{i\phi}UW_a$  for  $\phi \in \mathbb{R}$  and  $a \in \mathbb{Z}_2^{2n}$  induce the same symplectic transformation. In fact, the quotient of  $\text{Cl}_n$  up to the Pauli group and phase factors is isomorphic to  $\text{Sp}(2n, \mathbb{Z}_2)$ .

Thus, not only does the set of stabilizer states afford a transitive symmetry group, it is also true that the group has a geometric interpretation, in terms of symmetries of symplectic vector spaces. The geometric description of the Clifford group enables some explicit calculations that are crucial ingredients to our main result: Theorem 1. Indeed, this statement depends on an analysis of the representation theory of tensor powers of the Clifford group [69], which in turn relies on counting arguments involving orbits of tuples of vectors  $\langle v_1, \dots, v_k \rangle \in (\mathbb{Z}_2^{2n})^{\times k}$  under the action of  $\text{Sp}(2n, \mathbb{Z}_2^{2n})$  [35].

We feel that this lends credence to our earlier claim that their “rich geometric structure” makes stabilizer states into an ideal model measurement ensemble.

## E. Related groups and uses in other fields

The Pauli group discussed in this paper is strongly related to the *Heisenberg groups* and their *Weyl representations*. These appear in a number of fields. The literature

on this subject is vast and seems, unfortunately, to be quite disconnected. We will not describe a unifying theory here, but merely mention some examples and how they relate to this work.

A variant that is of importance in quantum mechanics, functional analysis [64], and time-frequency analysis [60] involves operators acting on  $L^2(\mathbb{R})$ , the set of square-integrable functions on the real line. One way to approach it is to start with operators  $P, Q$  that satisfy the *canonical commutation relations*

$$[Q, P] = i\mathbb{1}.$$

This relation makes the linear space spanned by  $P, Q$  into a Lie algebra. The elements of the associated Lie group are sometimes referred to as *Weyl operators* and parameterized as

$$W_{p,q} = e^{-i\frac{1}{2}pq} e^{ipQ} e^{iqP}$$

for  $(p, q) \in \mathbb{R}^2$ . The group law can be verified to be

$$W_a W_b = e^{i\frac{1}{2}[a,b]} W_{(a+b)},$$

for  $a, b \in \mathbb{R}^2$  and  $[\cdot, \cdot]$  the standard symplectic form on  $\mathbb{R}^2$ . This is clearly analogous to the corresponding law (8) for the Pauli group. The normalizer of the Weyl operators – i.e. the analogue of the Clifford group – is often called the *metaplectic group* and is related to the symplectic group  $\text{Sp}(\mathbb{R}^2)$  [64]. In time-frequency analysis, Weyl operators are usually known as *time-frequency shifts* and the metaplectic group is sometimes referred to as the *oscillator group* [60]. The relatives of stabilizer states are complex Gaussian vectors that play an important role e.g. in quantum optics [70, 71].

The Weyl operators act on functions  $\psi \in L^2(\mathbb{R})$  as

$$(W_{p,q}\psi)(x) = e^{-i\frac{1}{2}pq} e^{ipx} \psi(x - q). \quad (12)$$

This formula suggests a natural way to define discretized versions of the Weyl operators: Just re-interpret the numbers  $p, q, x$  as elements of  $\mathbb{Z}_d$  for some natural number  $d$  to obtain versions of  $W_{p,q}$  acting on  $L^2(\mathbb{Z}_d) \simeq \mathbb{C}^d$ . It turns out [72, 73] that the theory becomes slightly cleaner if one also changes the phase factor in (12) as

$$e^{-i\frac{1}{2}pq} \mapsto \tau^{pq}, \quad \tau := e^{\pi i(d^2+1)/d} = (-1)^d e^{\pi i/d}.$$

This procedure does, in fact, define unitary operators on  $\mathbb{C}^d$  (and recovers the Pauli operators  $\bar{\mathcal{P}}_1$  when setting  $d = 2$ ).

These discrete Weyl-Heisenberg operators are usually introduced from a different point of view. To state it, let  $\{e_1, \dots, e_d\}$  be the standard basis of  $\mathbb{C}^d$  and define

$$\begin{aligned} X : e_k &\mapsto e_{k+1}, \\ Z : e_k &\mapsto \omega_d^k e_k, \end{aligned}$$

where  $\omega_d = e^{i2\pi/d} = \tau^2$  is a  $d$ -th root of unity. Then the discrete Weyl-Heisenberg operators can also be written as

$$W_{p,q} = \tau^{pq} X^q Z^p. \quad (13)$$

These operators are also known as *generalized Pauli operators*.

Once again, one can define an associated Clifford group as the normalizer of these  $W_{p,q}$ 's and introduce stabilizer groups and states that are compatible with this structure.

Further related groups and applications come from coding theory. With every binary code, one can associate the *weight enumerator polynomial* whose coefficients encode the number of codewords of a given weight. For certain classes of self-dual codes, one can fairly easily see that these polynomials are invariant under an associated symmetry group [58]. The complex Clifford group used in this paper appears here, but also a real-valued variant, which is more commonly studied in this context [59]. In our language, the real Clifford group arises as the normalizer of the group generated by the real Pauli operators. This real group arises in many other contexts, e.g. as the symmetry group of the *Barnes-Wall lattice*. A good starting point to the literature covering this approach is the book [59] (in particular the Background section of their Chapter 6).

Given all these similarities, it is natural to ask whether the low-rank recovery results of the present paper can be adapted to these more general Clifford groups and stabilizer states.

For the set of Weyl operators that appear in (13), it seems clear that if similar results could be established, new techniques would have to be developed for this purpose. Indeed, our proof relies crucially on the representation theory of the fourth tensor power of the Clifford group [69, 74] to derive bounds on the 8th moments of random vectors sampled from orbits. It is known [35, 36] that the representation theory of the particular Clifford group studied here behaves differently from its cousins already for the third tensor power. What is more, there is a precise sense in which the moment bounds are worse for these more general stabilizer states: they fail to form a *complex projective 3-design* [37]. We refer to Section V below for an introduction of the design concept.

Deciding whether our results can be translated to the more general case despite these obstacles is an interesting open problem.

The situation might be better for the real Clifford group. Here, analogous representation-theoretic results to those proven in [69] in the complex case had been known for some time [59, 75].

Deciding whether our results can be translated to the more general case remains an interesting open problem.

### III. CONVEX LOW-RANK RECOVERY AND PHASELIFT

Here, we briefly review some basic facts from the theory of convex low-rank recovery. We refer to Ref. [43] for a more thorough introduction.

Building on ideas from *compressed sensing* [43], low rank matrix recovery aims at reconstructing unknown  $d \times d$  matrices  $X$  of rank  $r$  from few noisy linear measurements of the form

$$y_k = \text{tr}(A_k X) + \epsilon_k \quad 1 \leq k \leq m. \quad (14)$$

For simplicity, the present paper restricts attention to hermitian matrices  $X, A_k \in H_d$ —though we expect that standard constructions can be used to lift this assumption, see e.g. [54].

The measurement model (14) can be written more succinctly as

$$y = \mathcal{A}(X) + \epsilon,$$

where  $y = (y_1, \dots, y_m)^T \in \mathbb{R}^m$  represents the measurement data,  $\epsilon = (\epsilon_1, \dots, \epsilon_m)^T$  denotes additive noise corruption and  $\mathcal{A} : H_d \rightarrow \mathbb{R}^m$  is the measurement operator

$$\mathcal{A}(Z) = \sum_{k=1}^m \text{tr}(A_k Z) e_k,$$

with  $e_1, \dots, e_m$  being the standard basis of  $\mathbb{R}^m$ .

For many measurement models, it has been proven that low-rank matrices can be recovered efficiently using a constrained nuclear norm minimization:

$$\begin{aligned} & \underset{Z \in H_d}{\text{minimize}} && \|Z\|_1 \\ & \text{subject to} && \|\mathcal{A}(Z) - y\|_{\ell_q} \leq \eta, \quad 1 \leq q \leq \infty. \end{aligned} \quad (15)$$

Here,  $\eta \geq \|\epsilon\|_{\ell_q}$  is an upper bound on the noise corruption in (14) and the nuclear norm  $\|Z\|_1 = \sum_{k=1}^d |\lambda_k(Z)|$  corresponds to the  $\ell_1$ -norm of the vector of eigenvalues of  $Z$ . Analytic reconstruction guarantees for low rank matrix reconstruction via (15) have been established for  $m = Crd \text{polylog}(d)$  sufficiently random measurements [43, 49, 51, 54, 55].

Phase retrieval—i.e. the problem of recovering a complex vector  $x \in \mathbb{C}^d$  from measurements of the form (1)—can also be re-cast as a particular instance of matrix recovery:

$$y_k = |\langle a_k, x \rangle|^2 + \epsilon_k = \text{tr}(a_k a_k^* x x^*) + \epsilon_k. \quad (16)$$

This matrix formulation—expressing the quadratic relations on  $x$  in terms of linear relations on its outer product  $X = x x^*$ —is called a *lifting* [13, 76]. Because the unknown quantity is now represented by a rank-one matrix,  $X = x x^*$ , it is natural to use the convex reconstruction protocol (15) for recovery. This approach is called

*PhaseLift* and it has been shown that  $m = Cn \log(n)$  random Gaussian measurement vectors  $a_1, \dots, a_m \in \mathbb{C}^d$  suffice to guarantee that *PhaseLift* recovers an unknown vector  $x \in \mathbb{C}^d$ , up to a global phase factor, with high probability [14].

The matrices  $X = xx^*$  associated with *PhaseLift* are not only rank-one, but also positive semidefinite:  $X \geq 0$ . Using this additional constraint, one can reduce *PhaseLift* to a feasibility problem [15, 77]. For instance, already  $m = Cn$  Gaussian measurements suffice to reconstruct any  $x \in \mathbb{C}^d$  via solving

$$Z^\sharp = \underset{Z \geq 0}{\operatorname{argmin}} \|\mathcal{A}(Z) - y\|_{\ell_q} \quad (17)$$

with  $q = 1$  [15]. This reconstruction has an added benefit: it does not require an a priori noise bound  $\eta$  as additional input. The reconstruction error—measured in Frobenius norm  $\|Z\|_2 = \sqrt{\operatorname{tr}(Z^2)}$ —scales directly proportional to the true noise level [15]:

$$\|Z^\sharp - xx^*\|_2 \leq C_2 \frac{\|\epsilon\|_{\ell_1}}{m}.$$

Going to back from matrices to vectors, there exists a global phase  $\phi \in [0, 2\pi[$  such that the largest eigenvector  $z^\sharp$  of  $Z^\sharp$  obeys

$$\|z^\sharp - e^{i\phi}x\|_{\ell_2} \leq C_2 \min \left\{ \|x\|_{\ell_2}, \frac{\|\epsilon\|_{\ell_1}}{m\|x\|_{\ell_2}} \right\}$$

c.f. [15, Theorem 1.3].

These *PhaseLift* results can be generalized to cover recovery of hermitian matrices with higher rank. For instance, [21, Theorem 2] implies that with high probability  $m \geq Crn$  random Gaussian measurements  $A_k = a_k a_k^*$  suffice to reconstruct any hermitian rank- $r$  matrix  $X$  via (15). If  $X \in H_d$  is also positive semidefinite, then reconstruction may be done via (17) with  $1 \leq q \leq \infty$  [25, Theorem 4]. This reconstruction is not only stable with respect to noise corruption, but also robust towards the model assumption of low rank. The minimizer  $Z^\sharp$  of (17) obeys

$$\|Z^\sharp - X\|_2 \leq \frac{C_2}{\sqrt{r}} \sigma_r(X) + C_3 \frac{\|\epsilon\|_{\ell_q}}{m^{\frac{1}{q}}},$$

where

$$\sigma_r(X) = \inf \{\|X - Z\|_1 : \operatorname{rank}(Z) = r\} \quad (18)$$

is the nuclear norm error of the best rank- $r$  approximation to  $X$ .

#### IV. RESULTS: LOW-RANK RECOVERY FROM CLIFFORD ORBITS

In this work, we prove guarantees for low-rank recovery from Clifford orbits.

More precisely, set  $d = 2^n$  for some  $n$ , fix  $z \in \mathbb{C}^d$  with  $\|z\|_{\ell_2} = 1$  and let  $zz^*$  be the projection operator onto  $z$ . The Clifford orbits we are concerned with are the sets

$$\operatorname{Cl}_n \cdot zz^* = \{Uzz^*U^\dagger \mid U \in \operatorname{Cl}_n\}.$$

Sometimes, we find it advantageous to talk about the vectors  $Uz$ , rather than their projections. The two points of view are consistent if we set

$$\operatorname{Cl}_n \cdot z = \{Uz \mid U \in \operatorname{Cl}_n\} / \{e^{i\phi}\}_\phi,$$

where the quotient means that if two vectors differ by a phase  $U_1z = e^{i\phi}U_2z$ , we retain only one of them (equivalently: we work in projective space). These orbits are always finite.

The quality of the recovery guarantee depends on a measure of sparsity of the expansion coefficients of  $zz^*$  with respect to the Pauli basis. To state that measure, consider a general hermitian matrix  $Z$ . Then

$$Z = \sum_{a \in \mathbb{Z}_2^n} 2^{-n/2} (\operatorname{tr} W_a Z) W_a.$$

Thus, up to normalization constants, the expansion coefficients are given by the *characteristic function*<sup>3</sup>  $\Xi(Z) : \mathbb{Z}_2^n \rightarrow \mathbb{R}$  of  $Z$ . It is defined as

$$\Xi(Z)(a) := \operatorname{tr}(W_a Z), \quad a \in \mathbb{Z}_2^n. \quad (19)$$

(The same function is called the *spreading function* in time-frequency analysis [60, 61, 78, 79].)

Our bounds turn out to depend on the  $\ell_4$ -norm of this function:

$$\|\Xi(zz^*)\|_{\ell_4} = \left( \sum_{a \in \mathbb{Z}_2^n} (\operatorname{tr} W_a zz^*)^4 \right)^{1/4}. \quad (20)$$

The definition of the Clifford group as the normalizer of the Paulis implies that this quantity is constant along Clifford orbits. Smaller values of  $\|\Xi(zz^*)\|_{\ell_4}$  turn out to lead to better recovery guarantees. At the same time, the number of non-zero coefficients of the characteristic function is lower-bounded by  $d^2 \|\Xi(zz^*)\|_{\ell_4}^{-4}$ . In this sense, Clifford orbits are connected with good recovery guarantees only if their elements have a “spread out” or “dense” characteristic function.

More precisely, the following quantity

$$\kappa(z, r) := \left( \frac{r}{d} \|\Xi(zz^*)\|_{\ell_4}^4 + 1 \right)^2. \quad (21)$$

appears in the sampling rate of our main result.

<sup>3</sup> To explain the origina of the terminology, recall that in probability theory, the *characteristic function* is the Fourier transform of a probability distribution. The quantum analogue of a distribution is a *density operator* and the expansion of a density operator with respect to the Weyl-Heisenberg group plays an analogues role, in quantum probability theory, to the classical characteristic function (cf. e.g. [66, 70])

**Theorem 1** (Main Theorem, general version). *Let  $d = 2^n$  for some  $n \in \mathbb{N}$ ,  $z \in \mathbb{C}^d$  with  $\|z\|_{\ell_2} = 1$ , and  $1 \leq r \leq d$ . Choose*

$$m \geq C_1 \kappa(z, r) r d \log(d) \quad (22)$$

*measurements  $A_k = a_k a_k^*$  independently and uniformly at random from the Clifford orbit  $\text{Cl}_n \cdot z z^*$ . Then with probability at least  $1 - e^{-\frac{\gamma m}{\kappa(z, r)}}$  any hermitian rank- $r$  matrix can be recovered from these measurements in the following sense:*

*For every hermitian rank- $r$  matrix  $X$  and every  $q \in [1, \infty]$ , the minimizer  $Z^\sharp$  of the convex optimization problem (15) fulfills*

$$\|Z^\sharp - X\|_2 \leq \frac{C_2}{\sqrt{r}} \sigma_r(X) + C_3 \sqrt{\kappa(z, r)} d m^{-\frac{1}{q}} \eta \quad (23)$$

*where  $\eta$  is the noise bound from (15) and the approximation error  $\sigma_r(X)$  was defined in (18). Here,  $C_1, C_2, C_3$  denote sufficiently large constants and the constant  $\gamma$  is sufficiently small.*

Note that we have normalized the measurement vectors such that  $\|a_k\|_{\ell_2} = 1$ . Other normalization conventions are also common. For example, Gaussian random measurements have an expected length of  $\|a_k\|_{\ell_2} \simeq \sqrt{d}$ . If we drop this normalization restriction, the noise bound in (23) generalizes to

$$C_3 \sqrt{\kappa(z / \|z\|_{\ell_2}, r)} \frac{d}{\|z\|_{\ell_2}^2} m^{-\frac{1}{q}} \eta.$$

Using the Gaussian normalization, the noise bound becomes independent of the ambient dimension  $d$ .

We prove Theorem 1 by following techniques presented in [25]: we establish a strong notion of a matrix-valued null space property—see Definition 5 below—by invoking Mendelson’s Small Ball Method [23, 80, 81]. In order to do so, we employ recent insights about the fourth moments of the Clifford group. These are described in our companion paper [69].

Theorem 1 depends on the parameter  $\kappa(z, r)$ . According to Ref. [69] it obeys

$$\left( \frac{r}{d+1} + 1 \right)^2 \leq \kappa(z, r) \leq (r+1)^2 \quad (24)$$

and the upper bound is saturated for stabilizer states. Thus, Theorem 1 requires a sampling rate of

$$m \geq 2C_1 r^3 d \log(d)$$

for randomly chosen stabilizer state measurements. We believe that this worst case scaling in the rank parameter  $r$  is an artifact of the proof technique. In contrast to this, typical orbits  $\text{Cl}(z)$  obey [69]

$$\kappa(z, r) \leq \frac{6r}{d+1} + 1 \leq 7$$

and the impact of  $\kappa(z, r)$  on the sampling rate (22) is negligible.

As explained in Section III, if the matrices  $X$  are assumed to be positive semi-definite, one can sometimes use the convex optimization problem (17) instead of (15) for recovery. The most obvious advantage is that (17) does not require an estimate for the strength of the noise vector  $\epsilon$ . Our second main result makes this precise for Clifford orbit measurements.

**Theorem 2** (Main Theorem, PSD version). *The statements of Theorem 1 continue to hold under the following substitutions:*

- *The lower bound on the probability of success is weakened to  $1 - (d+1)e^{-\frac{\gamma m}{d+1}}$ .*
- *The statement ranges over Hermitian matrices  $X$  of rank  $r$ , which are in addition assumed to be positive-semidefinite.*
- *The reconstruction  $Z^\sharp$  is now given by the minimizer of the convex optimization problem in Eq. (17), for an arbitrary choice of  $q \in [1, \infty]$ .*
- *The number  $\eta$  in (23) is replaced by  $\|\epsilon\|_{\ell_q}$ , the true noise strength, with  $q$  the same as above.*

Explicit bounds on the constants  $C_1, C_2, C_3, \gamma$  that appear in the two main theorems can in principle be extracted from our proofs. If one is only interested in the statement of Theorem 1 alone (as opposed to both Theorem 1 and Theorem 2), the constants improve somewhat.

Phase retrieval via PhaseLift is a particular case of matrix reconstruction, where  $X = x x^*$  is both positive semidefinite and rank-one. In this case, the bound in (24) becomes  $\kappa(z, 1) \leq 4$  and Theorem 2 implies the following statement:

**Corollary 1** (PhaseLift with Clifford orbit measurements). *Let  $d = 2^n$  and  $z \in \mathbb{C}^d$  with  $\|z\|_{\ell_2} = \sqrt{d}$ . Choose*

$$m \geq 4C_1 d \log(d) \quad (25)$$

*vectors  $a_1, \dots, a_m$  uniformly and independently at random from Clifford orbit  $\text{Cl}_n \cdot z$ .*

*Then with probability at least  $1 - d e^{-\frac{\gamma m}{4d}}$ , the phase retrieval problem (1) is well-posed in the following sense: For every  $x \in \mathbb{C}^d$  and every  $q \in [1, \infty]$ , the leading eigenvector  $z^\sharp$  of the minimizer  $Z^\sharp$  of Eq. (17) fulfills*

$$\min_{\phi \in [0, 2\pi)} \|z^\sharp - e^{i\phi} x\|_{\ell_2} \leq 2C_3 \min \left\{ \|x\|_{\ell_2}, \frac{\|\epsilon\|_{\ell_q}}{m^{1/q} \|x\|_{\ell_2}} \right\}.$$

Up to a single log-factor in the sampling rate  $m$ , and a weaker bound on the probability of failure, Corollary 1 reproduces [15, Theorem 1.3]—the strongest recovery guarantee for PhaseLift with Gaussian measurements we are aware of. We have chosen the particular



normalization  $\|z\|_{\ell_2} = \sqrt{d}$  to match the typical scaling of Gaussian random vectors and facilitate a direct comparison with Ref. [15]. Corollary 1 provides a theoretical justification for our prior numerical observation that random stabilizer measurements show close-to-optimal behavior as measurements for phase retrieval [16, Section 2].

We do not know whether the log-factor in Eq. (25) is necessary or not. In the case of Pauli measurements, one can prove the necessity of a log-factor by considering the recovery of stabilizer states [54, Theorem 15]. This suggests trying to establish a lower bound on  $m$  by analyzing the recovery of stabilizer states under stabilizer measurements. However, heuristic arguments (Appendix VII) indicate that this strategy is bound to fail. We therefore leave it as an open problem to determine whether or not the scaling of the sampling rate  $m$  can be made linear in the dimension  $d$ , or whether a logarithmic correction is required.

## V. MOMENTS OF GROUP ORBITS

Our results make use of representation theory to proof recovery guarantees for measurements that are sampled from group orbits. While we apply it only to the Clifford group, the technique is more general than that. In this section, we introduce the underlying concepts.

In our analysis of the probabilistic construction of the measurement operator  $\mathcal{A}$ , we will make essential use of finite moments of the random vectors  $a_k$ . Here, we define the  $2t$ -th moments of a random vector  $a \in \mathbb{C}^d$  as

$$\mathbb{E} [a^{\otimes t} (a^*)^{\otimes t}] \quad (26)$$

(we will not make use of moments of odd degree.) To give an example, we consider the cases where  $a$  is a random Gaussian, or a vector drawn uniformly from the unit-sphere in  $\mathbb{C}^d$ . In these cases, there is a simple, explicit expression for the moments. Indeed, let  $S_t$  be the symmetric group on  $t$  symbols and consider its representation on  $(\mathbb{C}^d)^{\otimes t}$  by permuting tensor factors:

$$\pi x_1 \otimes \cdots \otimes x_t = x_{\pi_1} \otimes \cdots \otimes x_{\pi_t}, \quad \forall x_k \in \mathbb{C}^d, \pi \in S_t.$$

Let  $\text{Sym}^t(\mathbb{C}^d)$  be the *totally symmetric subspace*, i.e. the subspace of  $(\mathbb{C}^d)^{\otimes t}$  on which  $S_t$  acts trivially. Let  $P_{[t]}$  be the orthogonal projection onto it. It is clear that  $a^{\otimes t} \in \text{Sym}^t(\mathbb{C}^d)$  with probability one. Therefore, the  $2t$ -th moments as defined in Eq. (26) is a Hermitian operator with support in  $\text{Sym}^t(\mathbb{C}^d)$ . For Gaussian or uniform random vectors, one can show (see below) that it is, in fact, proportional to the projection onto the totally symmetric subspace:

$$\mathbb{E} [a^{\otimes t} (a^*)^{\otimes t}] = c_t P_{[t]}, \quad (27)$$

with normalization constant

$$c_t = \frac{\mathbb{E} [\|a\|_{\ell_2}^{2t}]}{\dim \text{Sym}^t(\mathbb{C}^d)}.$$

Often, one can cast the analysis of randomized constructions into a form that only makes use of  $2t$ -th moments up to some finite value of  $t$ . This has been used in particular for the analysis of PhaseLift [16, 21, 32]. The strongest result, established in Ref. [21], shows that any random vector whose 4-th moments match the ones of vectors drawn uniform from the sphere, performs essentially optimally for PhaseLift. Such ensembles have a name [29, 30]:

**Definition 4.** A random vector  $a \in \mathbb{C}^d$  taking values on the complex unit-sphere is called a *complex projective  $t$ -design* if its  $2t$ -th moment is proportional to the projection  $P_{[t]}$  onto the totally symmetric subspace.

With the relevance of moment calculations for phase retrieval established, it is natural to ask how to identify natural random vectors whose moments can be computed. A simple but powerful approach to this problem is to relate moments to symmetries [82].

Indeed, assume that  $a$  is drawn from some set  $S \subset \mathbb{C}^d$ . Let  $G$  be a subgroup of the unitary group  $U(d)$  such that the distribution on  $S$  is  $G$ -invariant (if  $S$  is finite and  $a$  is drawn uniformly from  $S$ , this just means that  $G$  acts on  $S$ ). Then clearly, for every  $U \in G$ , the operator  $U^{\otimes t}$  commutes with  $\mathbb{E} [a^{\otimes t} (a^*)^{\otimes t}]$ . This allows us to invoke Schur's Lemma: Let

$$\text{Sym}^t(\mathbb{C}^d) = \bigoplus_{\lambda} V_{\lambda} \otimes \mathbb{C}^{d_{\lambda}}$$

be the decomposition of  $\text{Sym}^t(\mathbb{C}^d)$  into irreps  $V_{\lambda}$  of  $G$  with multiplicity  $d_{\lambda}$ . Then Schur's Lemma says that

$$\mathbb{E} [a^{\otimes t} (a^*)^{\otimes t}] = \bigoplus_{\lambda} P_{\lambda} \otimes B_{\lambda}, \quad (28)$$

where  $P_{\lambda}$  is the identity on  $V_{\lambda}$  and  $B_{\lambda}$  a suitable matrix acting on the multiplicity space  $\mathbb{C}^{d_{\lambda}}$ . If all irreps are non-degenerate, i.e.  $d_{\lambda} = 1 \forall \lambda$ , the expression simplifies to

$$\mathbb{E} [a^{\otimes t} (a^*)^{\otimes t}] = \bigoplus_{\lambda} \beta_{\lambda} P_{\lambda}, \quad (29)$$

for suitable  $\beta_{\lambda} \in \mathbb{C}$ . This turns out to be the case for the groups we are interested in.

This analysis allows us to give a one-line proof of Eq. (27): The formula follows from the fact that the Gaussian and the Haar distribution are invariant under  $U(d)$  and that  $U(d)$  acts irreducibly on  $\text{Sym}^t(\mathbb{C}^d)$  for every  $t, d$ .

More generally: Let  $G \subset U(d)$  be a group such that  $G$  acts irreducibly on  $\text{Sym}^t(\mathbb{C}^d)$ . Then by the above discussion, the orbit of any normalized vector  $z \in \mathbb{C}^d$

under  $G$  is a complex projective 4-design and therefore, Ref. [21] establishes near-perfect recovery guarantees for PhaseLift with measurements sampled from this orbit. (Ref. [16] gives weaker results, but makes non-trivial statements already for 3-designs.)

The analysis in Ref. [21] uses 4-th moments to establish certain large-deviation bounds on quantities associated with the random vectors. If a random vector  $a$  fails to be a 4-design, these arguments cannot be used directly. However, the technical premise of this paper is that the proofs can sometimes be adapted. Indeed, if the measurement ensemble affords a symmetry group that is sufficiently large such that  $\text{Sym}^4(\mathbb{C}^d)$  decomposes into few, simple, and ideally non-degenerate representation spaces, then it might be feasible to bound all necessary quantities from Eqs. (28), (29).

Motivated by this, the present authors were part of a collaboration that computed the representation theory of the Clifford group acting on  $\text{Sym}^4(\mathbb{C}^d)$  [69]. While it was already known that the action could not be irreducible [35–37], the “second best” scenario turned out to be realized: There are only two, non-degenerate irreducible representations. What is more, there is a simple description of these irreps. The results from [69] required in this paper are summarized in the following theorem:

**Theorem 3 ([69]).** *Let  $d = 2^n$  and let  $P_{[4]}$  denote the projector onto the totally symmetric subspace  $\text{Sym}^4(\mathbb{C}^d)$ . Let*

$$Q = \frac{1}{d^2} \sum_{a \in \mathbb{Z}_2^n} W_a^{\otimes 4}$$

and define

$$P_+ = P_{[4]}Q, \quad P_- = P_{[4]}(1 - Q). \quad (30)$$

Then  $\{P_+, P_-\}$  are the projections onto the irreducible representations of  $\text{Cl}_n$  within  $\text{Sym}^4(\mathbb{C}^d)$ .

In particular, if  $a$  is drawn uniformly from a Clifford orbit  $\text{Cl}_n \cdot z$  with  $\|z\|_{\ell_2} = 1$ , it holds that

$$\mathbb{E} [a^{\otimes t} (a^*)^{\otimes t}] = \beta_+(z)P_+ + \beta_-(z)P_-, \quad (31)$$

with coefficients

$$\begin{aligned} \beta_+(z) &= \frac{6}{(d+2)(d+1)d^2} \|\Xi(zz^*)\|_{\ell_4}^4, \\ \beta_-(z) &= \frac{24 \left(1 - \frac{1}{d^2} \|\Xi(zz^*)\|_{\ell_4}^4\right)}{(d+4)(d+2)(d+1)(d-1)}. \end{aligned}$$

The dependency of the coefficients  $\beta_{\pm}(z)$  on the characteristic function is the ultimate reason for  $\Xi(zz^*)$  appearing in the sampling rate  $m$  of Theorem 1 through  $\kappa(z, r)$ . To compare the situation to 4-designs, we borrow the bound

$$\frac{2d}{(d+1)} \leq \|\Xi(zz^*)\|_{\ell_4}^4 \leq d \quad \forall z \in \mathbb{C}^d : \|z\|_{\ell_2} = 1 \quad (32)$$

from Ref. [69]. It includes the special case  $\|\Xi(zz^*)\|_{\ell_4}^4 = \frac{4d}{(d+3)}$ , which is indeed attained for certain  $z$ 's [69]. One verifies that for this value, the coefficients coincide:  $\beta_+(z) = \beta_-(z) = \binom{d+3}{4}^{-1}$ . Using  $P_+ + P_- = P_{[4]}$ , this implies that Eq. (31) reduces to the defining property of a 4-design. Hence, the strong recovery results from [21, 25] apply to these specific orbits.

However, for general orbits,  $\beta_+(z)$  and  $\beta_-(z)$  do not coincide. Stabilizer states are an extreme case, in the sense that they saturate the upper bound presented in (32) [69], which in turn implies that the difference between  $\beta_+(z)$  and  $\beta_-(z)$  is maximal. For such orbits, we obtain the weakest results, in that the oversampling factor  $\kappa(z, r)$  in Theorem 1 becomes largest. Fortunately, the adverse scaling of  $\kappa(z, r)$  does not become relevant for bounded rank  $r$ . In particular, our results on phase retrieval ( $r = 1$ ) are near-optimal for all Clifford orbits (c.f. Corollary 1).

Finally, we mention again that the deviation between the moments of Clifford orbits and of uniform random vectors first occurs for  $t = 4$ . Clifford orbits have recently been proven [35–37] to form are known to form complex projective  $t$ -designs for  $t = 1, 2, 3$ .

## VI. PROOFS

Our proof strategy is as follows: We aim to establish a robust *Null Space Property* for measurement operators  $\mathcal{A}$  comprised of random elements of a Clifford orbit. Roughly speaking, this means that no low-rank matrix is contained in the kernel (or null space) of  $\mathcal{A}$ . To do so, we follow the proof technique of Ref. [25] and invoke a now-well-known tool called *Mendelson's Small Ball Method* [23, 80, 81]. This statement depends on certain concentration properties of the measurements  $A_k = a_k a_k^*$ . These, in turn, are derived from representation theoretic data of the Clifford group, most notably Theorem 3.

The remainder of this section is organized as follows:

1. In Section VIA we recall the definition of the Null Space Property, as well as Mendelson's Small Ball Method.
2. Section VIB shows how relevant concentration parameters of the measurements can be derived from the representation theory of their symmetry group.
3. The main work is done in Section VIC, where we combine these ingredients to prove a Null Space Property for Clifford orbits.
4. In Section VID we use this Null Space Property to derive our first main result: Theorem 1.
5. Finally, Section VIE generalizes our findings to positive-semidefinite matrix recovery (Theorem 2).

### A. The robust Null Space Property and Mendelson's Small Ball Method

The notion of a *Null Space Property* is somewhat folklore in the field of compressed sensing, see e.g. [43] for a discussion of its origin. One can define analogous properties for matrix reconstruction [25, 83–86]. Roughly speaking, a measurement operator  $\mathcal{A} : H_d \rightarrow \mathbb{R}^m$  obeys a null space property of order  $r$ , if no rank- $r$  matrix is contained in the kernel, or nullspace, of  $\mathcal{A}$ . This is a necessary criterion for *uniform* rank- $r$  matrix recovery, where uniform means that all matrices of rank  $r$  or less, can be reconstructed:

**Definition 5** (Definition 3.1 in [25] for hermitian matrices). For fixed  $r$  and  $q \geq 1$ , a measurement operator  $\mathcal{A} : H_d \rightarrow \mathbb{R}^m$  obeys the  $\ell_q$ -robust Null Space Property of order  $r$  ( $r/\ell_q$ -NSP) with constants  $\rho \in (0, 1)$  and  $\tau > 0$ , if

$$\|Z_r\|_2 \leq \frac{\rho}{\sqrt{r}} \|Z_c\|_1 + \tau \|\mathcal{A}(Z)\|_{\ell_q} \quad \forall Z \in H_d. \quad (33)$$

Here  $Z_r = \operatorname{argmin}_{\operatorname{rank}(Y)=r} \|Y - Z\|_1$  denotes the minimizer of the approximation error  $\sigma_r(Z)$  in (18) and  $Z_c = Z - Z_r$  obeys  $\|Z_c\|_1 = \sigma_r(Z)$ .

Validity of a  $r/\ell_q$ -NSP implies that any matrix  $Z$  with rank at most  $r$  obeys  $\|Z\|_2 \leq \tau \|\mathcal{A}(Z)\|_{\ell_q}$  and therefore does not lie in  $\mathcal{A}$ 's null space. While this is clearly necessary for uniform rank- $r$  matrix recovery, it is also sufficient, c.f. [25, Theorem 3.3]. We will use this assertion to derive Theorem 1 in Section VID.

Note that (33) is invariant under scaling and we may set  $\|Z\|_2 = 1$  without loss of generality. Moreover, any normalized matrix  $Z \in H_d$  which also obeys  $\|Z_r\|_2 \leq \frac{\rho}{\sqrt{r}} \|Z_c\|_1$  fulfills (33), irrespective of  $\mathcal{A}$ . So, when aiming to establish a  $r/\ell_q$ -NSP for any particular  $\mathcal{A}$ , we may restrict our attention to

$$T_{\rho,r} = \left\{ Z \in H_d : \|Z_r\|_2 > \frac{\rho}{\sqrt{r}} \|Z_c\|_1, \|Z\|_2 = 1 \right\}. \quad (34)$$

In turn,  $\mathcal{A} : H_d \rightarrow \mathbb{R}^m$  obeys the  $r/\ell_q$ -NSP with constants  $\rho \in (0, 1)$  and  $\tau > 0$ , if

$$\inf_{Z \in T_{\rho,r}} \|\mathcal{A}(Z)\|_{\ell_q} \geq \frac{1}{\tau}. \quad (35)$$

Note that the parameters  $r, \rho$  implicitly feature in the definition of  $T_{\rho,r}$ , while  $\tau$  is inversely proportional to the best lower bound achievable in (35).

Our NSP-proof is based on the following statement [23, 80, 81].

**Theorem 4** (Variant of Mendelson's small ball method<sup>4</sup>). Fix  $E \subset \mathbb{R}^d$  and let  $\phi_1, \dots, \phi_m \in \mathbb{R}^d$  be independent copies

of a random vector  $\phi$ . For  $\xi > 0$  define

$$Q_\xi(E; \phi) = \inf_{z \in E} \Pr[|\langle \phi, z \rangle| \geq \xi], \quad \text{and} \quad (36)$$

$$W_m(E; \phi) = \mathbb{E} \left[ \sup_{z \in E} \langle h, z \rangle \right] \quad \text{with} \quad (37)$$

$$h = \frac{1}{\sqrt{m}} \sum_{k=1}^m \varepsilon_k \phi_k \in \mathbb{R}^d, \quad (38)$$

where each  $\varepsilon_k$  is an independent instance of a Rademacher random variable (i.e.  $\varepsilon_k$  assumes  $+1$  and  $-1$  with equal probability). Then for any  $\xi > 0$  and  $t \geq 0$ , the following bound is true with probability at least  $1 - e^{-2t^2}$ :

$$\frac{1}{\sqrt{m}} \inf_{z \in E} \sum_{k=1}^m |\langle \phi_k, z \rangle| \geq \xi \sqrt{m} Q_{2\xi}(E; \phi) - 2W_m(E; \phi) - \xi t.$$

In this work, we will employ the following corollary:

**Corollary 2.** Fix  $r, \rho$  and let  $T_{\rho,r} \subset H_d$  be the set introduced in (34). Suppose that  $\mathcal{A} : H_d \rightarrow \mathbb{R}^m$  is a measurement operator containing  $m$  independent instances of a single random matrix  $A \in H_d$  as individual measurements. Then for any  $q \geq 1$ ,  $\xi > 0$  and  $t \geq 0$

$$\inf_{Z \in T_{\rho,r}} \|\mathcal{A}(Z)\|_{\ell_q} \geq m^{\frac{1}{q}-\frac{1}{2}} (\xi \sqrt{m} Q_{2\xi}(T_{\rho,r}; A) - 2W_m(T_{\rho,r}, A) - \xi t) \quad (39)$$

is true with probability at least  $1 - e^{-2t^2}$ . Here  $Q_{2\xi}(T_{\rho,r}; A)$  and  $W_m(T_{\rho,r}, A)$  are the parameters defined in (36) and (37).

*Proof.*  $H_d$  is a real-valued vector space isomorphic to  $\mathbb{R}^{d^2}$  and we may identify each  $A_k$  with an instance  $\phi_k$  of the random vector  $A := \phi \in \mathbb{R}^{d^2} \simeq H_d$ . Also, the Frobenius inner product  $(Y, Z) = \operatorname{tr}(YZ)$  endows  $H_d$  with an inner product. Setting  $E = T_{\rho,r} \subset H_d \simeq \mathbb{R}^{d^2}$ , where  $T_{\rho,r}$  was defined in (34) and applying Theorem 4 yields

$$\inf_{Z \in T_{\rho,r}} \frac{1}{\sqrt{m}} \sum_{k=1}^m |(A_k, Z)| = \inf_{Z \in T_{\rho,r}} \frac{1}{\sqrt{m}} \|\mathcal{A}(Z)\|_{\ell_1}.$$

Finally, we employ the basic norm inequality  $\|z\|_1 \leq m^{1-\frac{1}{q}} \|z\|_{\ell_q} \quad \forall z \in \mathbb{R}^m, \quad \forall q \geq 1$  (see for instance [43, Equation A.3]) to conclude

$$\inf_{Z \in T_{\rho,r}} \|\mathcal{A}(Z)\|_{\ell_q} \geq m^{\frac{1}{q}-\frac{1}{2}} \inf_{Z \in T_{\rho,r}} \frac{1}{\sqrt{m}} \|\mathcal{A}(Z)\|_{\ell_1}.$$

□

a lower bound on  $\inf_{z \in E} \sqrt{\sum_{k=1}^m |\langle \phi_k, z \rangle|^2}$ , while this statement is slightly stronger, as it bounds  $\frac{1}{\sqrt{m}} \inf_{z \in E} \sum_{k=1}^m |\langle \phi_k, z \rangle|$  instead. This stronger claim, however, is also implied by Mendelson's original proof, see for instance [25, Remark 5.1].

<sup>4</sup> We remark that Mendelson's small ball method often refers to

### B. Bounding the relevant parameters in Corollary 2 for Clifford orbits

Two parameters feature prominently in Corollary 2:  $W_m(T_{\rho,r}; A)$  defined in (37) and  $Q_{2\xi}(T_{\rho,r}; A)$  defined in (36). Both parameters crucially depend on the geometry of  $T_{\rho,r} \subseteq H_d$  introduced in (34) and the distribution of the measurement matrices  $A = aa^*$ . In our case, these are uniformly selected from a Clifford orbit  $\text{Cl}_n \cdot zz^*$ .

A first auxiliary statement addresses the geometry of  $T_{\rho,r}$  and asserts that the *effective rank* of every  $T_{\rho,r}$  cannot be too large:

**Lemma 1.** *Let  $T_{\rho,r} \subset H_d$  be the set introduced in (34) for some  $\rho \in (0, 1)$  and  $1 \leq r \leq d$ . Then*

$$\frac{\|Z\|_1^2}{\|Z\|_2^2} \leq \left(\frac{\rho+1}{\rho}\right)^2 r \quad \forall Z \in T_{\rho,r}. \quad (40)$$

*Proof.* Combining  $\|Z_r\|_1 \leq \sqrt{r}\|Z_r\|_2$  with the defining property of  $Z \in T_{\rho,r}$  reveals

$$\|Z\|_1 \leq \|Z_r\|_1 + \|Z_c\|_1 \leq \frac{\rho+1}{\rho} \sqrt{r}\|Z_r\|_2,$$

and the claim follows from  $\|Z_r\|_2 \leq \|Z\|_2 = 1$ .  $\square$

This insight allows one to bound the first parameter featuring in Corollary 2:

**Proposition 4.** *Fix  $d = 2^n$  and suppose that  $A = aa^*$  results from choosing an element of a Clifford orbit  $\text{Cl}_n \cdot zz^*$  with  $\|z\|_{\ell_2} = 1$  uniformly at random. Also, fix  $1 \leq r \leq d$ ,  $\rho \in (0, 1)$  and suppose  $m \geq 2d \log(d)$ . Then*

$$W_m(T_{\rho,r}; A) \leq \frac{6.2098}{\rho} \sqrt{\frac{r \log(2d)}{d+1}}.$$

*Proof.* This proof closely resembles a comparable analysis provided in [21]. Matrix Hoelder together with Lemma 1 implies

$$\begin{aligned} W_m(T_{\rho,r}; A) &= \mathbb{E} \left[ \sup_{Z \in T_{\rho,r}} (H, Z) \right] \leq \sup_{Z \in T_{\rho,r}} \|Z\|_1 \mathbb{E} [\|H\|_\infty] \\ &\leq \frac{\rho+1}{\rho} \sqrt{r} \mathbb{E} [\|H\|_\infty] \leq \frac{2}{\rho} \sqrt{r} \mathbb{E} [\|H\|_\infty], \end{aligned}$$

with  $H = \frac{1}{\sqrt{m}} \sum_{k=1}^m \epsilon_k a_k a_k^*$ . Each  $A_k = a_k a_k^*$  obeys  $\mathbb{E}[A_k] = \frac{1}{d} \mathbb{I}$ , because it is uniformly chosen from a Clifford orbit (Formula (27) for  $t = 1$ ). This property alone together with the Rademacher randomness in  $H$  allows for bounding  $\mathbb{E}[\|H\|_\infty]$  by combining a non-commutative Khintchine inequality with a matrix Chernoff bound, see for instance [21, Proposition 13]. Adapting said statement to unit normalization ( $\|a_k\|_{\ell_2} = \|z\|_{\ell_2} = 1$ ) implies

$$\mathbb{E} [\|H\|_\infty] \leq 3.1049 \sqrt{\frac{\log(2d)}{d+1}},$$

provided that  $m \geq 2d \log(d)$  and the claim readily follows.  $\square$

Establishing a lower bound on the remaining parameter  $Q_\xi(T_{\rho,r}; aa^*)$  for Clifford orbits is considerably more challenging. We do so by applying a Paley-Zygmund inequality that depends on the following auxiliary statement.

**Lemma 2.** *Fix  $Z \in H_d$  and define the random variable  $S_Z := \langle a, Za \rangle$ , where  $a$  is uniformly chosen from a Clifford orbit  $\text{Cl}_n \cdot zz^*$  with  $\|z\|_{\ell_2} = 1$ . Then*

$$\mathbb{E} [S_Z^2] = \frac{(\|Z\|_2^2 + \text{tr}(Z)^2)}{(d+1)d} \quad \text{and} \quad (41)$$

$$\mathbb{E} [S_Z^4] \leq \left( \frac{6}{d} \|\Xi(zz^*)\|_{\ell_4}^4 \frac{\|Z\|_1^2}{\|Z\|_2^2} + 13 \right) \mathbb{E} [S_Z^2]^2. \quad (42)$$

*Proof.* Equation (41) is a consequence of the fact that Clifford orbits obey Formula (27) for  $t = 2$ :

$$\begin{aligned} \mathbb{E} [S_Z^2] &= \mathbb{E} [\langle a, Za \rangle^2] = \mathbb{E} [\text{tr}(aa^* Z^2)] \\ &= \text{tr} \left( \mathbb{E} [a^{\otimes 2} (a^*)^{\otimes 2}] Z^{\otimes 2} \right) \\ &= \frac{2 \text{tr} (P_{\text{Sym}^2} Z^{\otimes 2})}{(d+1)d} = \frac{\text{tr}(Z^2) + \text{tr}(Z)^2}{(d+1)d}. \end{aligned}$$

The last equality follows from applying standard techniques from multilinear algebra, see e.g. [16, Lemma 6], or [21, Lemma 17].

Deriving the fourth moment bound (42) is more involved. For any  $Z \in H_d$  Theorem 3 implies

$$\begin{aligned} \mathbb{E} [S_Z^4] &= \mathbb{E} [\langle a, Za \rangle^4] = \text{tr} \left( \mathbb{E} [a^{\otimes 4} (a^*)^{\otimes 4}] Z^{\otimes 4} \right) \\ &= \beta_+(z) \text{tr} (P_+ Z^{\otimes 4}) + \beta_-(z) \text{tr} (P_- Z^{\otimes 4}). \end{aligned}$$

We can use  $P_+ = P_{[4]}Q$  and  $P_- = P_{[4]}(1 - Q)$  with  $Q = \frac{1}{d^2} \sum_{a \in \mathbb{Z}_2^n} W_a^{\otimes 4}$  to rewrite this expression as

$$\begin{aligned} \mathbb{E} [S_Z^4] &= (\beta_+(z) - \beta_-(z)) \text{tr} (P_{[4]} Q Z^{\otimes 4}) \\ &\quad + \beta_-(z) \text{tr} (P_{[4]} Z^{\otimes 4}). \end{aligned} \quad (43)$$

The second trace expression can be explicitly computed, e.g. by adapting the argument of [21, Lemma 17]:

$$\begin{aligned} &24 \left| \text{tr} (P_{\text{Sym}^4} Z^{\otimes 4}) \right| \\ &= \left| \text{tr}(Z)^4 + 8 \text{tr}(Z) \text{tr}(Z^3) + 3 \text{tr}(Z^2)^2 \right. \\ &\quad \left. + 6 \text{tr}(Z)^2 \text{tr}(Z^2) + 6 \text{tr}(Z^4) \right| \\ &\leq 3 \left( \text{tr}(Z)^2 + \text{tr}(Z^2) \right)^2 + 8 |\text{tr}(Z)| \|Z\|_2^3 + 6 \|Z\|_2^4 \\ &\leq 3 \left( \text{tr}(Z)^2 + \|Z\|_2^2 \right)^2 + 4 \left( \text{tr}(Z)^2 + \|Z\|_2^2 \right) \|Z\|_2^2 + 6 \|Z\|_2^4 \\ &\leq 13 \left( \text{tr}(Z)^2 + \|Z\|_2^2 \right)^2. \end{aligned}$$



Here, we have used standard Schatten- $p$  norm inequalities such as  $\text{tr}(Z^3) \leq \|Z\|_3^3 \leq \|Z\|_2^3$  and  $\text{tr}(Z^4) = \|Z\|_4^4 \leq \|Z\|_2^4$  as well as the AM-GM inequality:  $|\text{tr}(Z)| \|Z\|_2 \leq \frac{1}{2} (\text{tr}(Z)^2 + \|Z\|_2^2)$ .

We start bounding the remaining trace expression by noticing

$$\begin{aligned} \left| \text{tr} \left( P_{[4]} Q Z^{\otimes 4} \right) \right| &\leq \text{tr} \left( P_{[4]} Q |Z|^{\otimes 4} \right) \leq \text{tr} \left( Q |Z|^{\otimes 4} \right) \\ &= \frac{1}{d^2} \sum_{a \in \mathbb{Z}_2^n} \left( W_a^{\otimes 4}, |Z|^{\otimes 4} \right) \\ &= \frac{1}{d^2} \sum_{a \in \mathbb{Z}_2^n} (W_a, |Z|)^4. \end{aligned}$$

Here  $|Z| = \sqrt{ZZ^*}$  denotes the matrix absolute value of  $Z$  and the inequalities above are standard relations for positive-semidefinite matrices. Applying matrix Hoelder and using the fact that Schatten- $p$ -norms of  $Z$  and  $|Z|$  coincide by definition allows us to deduce

$$\begin{aligned} \frac{1}{d^2} \sum_{a \in \mathbb{Z}_2^n} (W_a, |Z|)^4 &\leq \frac{1}{d^2} \sum_{a \in \mathbb{Z}_2^n} \|W_a\|_\infty^2 \|Z\|_1^2 (W_a, |Z|)^2 \\ &= \frac{\|Z\|_1^2}{d^2} \sum_{a \in \mathbb{Z}_2^n} (W_a, |Z|)^2 = \frac{\|Z\|_1^2 \|Z\|_2^2}{d}. \end{aligned}$$

The second line is due to the fact that Pauli matrices are a unitary ( $\|W_a\|_\infty = 1$ ) matrix basis of  $H_d$  that is orthogonal with respect to the Frobenius inner product ( $(W_a, W_b) = d\delta_{a,b}$ ).

We can now move on to bound pre-factors. Formula (32) implies

$$\begin{aligned} \beta_-(z) &\leq \frac{24 \left( 1 - \frac{2}{(d+1)d} \right)}{(d+4)(d+2)(d+1)(d-1)} \\ &= \frac{24}{(d+4)(d+1)^2 d} \leq \frac{24}{(d+1)^2 d^2}, \end{aligned}$$

as well as

$$\begin{aligned} |\beta_+(z) - \beta_-(z)| &= \frac{|d^2 + 3d - 4d^2 / \|\Xi(zz^*)\|_{\ell_4}^4|}{(d+4)(d-1)} \beta_+(z) \\ &\leq \frac{d\beta_+(z)}{(d+4)} \leq \frac{6\|\Xi(zz^*)\|_{\ell_4}^4}{(d+1)^2 d^2} \end{aligned}$$

Inserting all these individual bounds into (43) implies

$$\begin{aligned} \mathbb{E} \left[ S_Z^4 \right] &\leq |\beta_+(z) - \beta_-(z)| \left| \text{tr} \left( P_{[4]} Q Z^{\otimes 4} \right) \right| \\ &\quad + |\beta_-(z)| \left| \text{tr} \left( P_{[4]} Z^{\otimes 4} \right) \right| \\ &\leq \frac{6\|\Xi(zz^*)\|_{\ell_4}^4 \|Z\|_1^2 \|Z\|_2^2}{(d+1)d^3} + \frac{13(\text{tr}(Z)^2 + \|Z\|_2^2)^2}{(d+1)^2 d^2} \\ &\leq \left( \frac{6}{d} \|\Xi(zz^*)\|_{\ell_4}^4 \frac{\|Z\|_1^2}{\|Z\|_2^2} + 13 \right) \left( \frac{\text{tr}(Z)^2 + \|Z\|_2^2}{(d+1)d} \right)^2 \end{aligned}$$

and the claim follows.  $\square$

The pre-factor in the 4-th moment bound (42) depends both on the characteristic function  $\Xi(zz^*)$  and the effective rank of  $Z$ . However, without putting further restrictions on  $Z$  and the Clifford orbit, this is unavoidable up to multiplicative constants: Choosing  $z = \psi \in \mathbb{C}^d$  to be a stabilizer state and setting  $Z = W_a$  ( $a \neq 0 \in \mathbb{Z}_2^n$ ) results in

$$\begin{aligned} \mathbb{E} \left[ S_{W_a}^4 \right] &= (d+1) \mathbb{E} \left[ S_{W_a}^2 \right]^2 \\ &= \left( \frac{1}{d} \|\Xi(\psi\psi^*)\|_{\ell_4}^4 + 1 \right) \mathbb{E} \left[ S_{W_a}^2 \right]^2. \end{aligned}$$

**Proposition 5.** Fix  $d = 2^n$  and let  $A = aa^*$  be a randomly chosen element of a Clifford orbit  $\text{Cl}_n \cdot zz^*$ . Then the parameter  $Q_\xi(T_{\rho,r}, A)$ , featuring in Corollary 2, obeys

$$Q_\xi(T_{\rho,r}, A) \geq \frac{\rho^2}{24\sqrt{\kappa(z,r)}} \left( 1 - \left( \sqrt{(d+1)d\xi} \right)^2 \right)^2,$$

where  $\kappa(z,r)$  was introduced in (21). This bound is true for any  $0 \leq \xi \leq \frac{1}{\sqrt{(d+1)d}}$ ,  $1 \leq r \leq d$  and  $\rho \in (0,1)$ .

*Proof.* Fix  $Z \in T_{\rho,r}$ ,  $\xi \geq 0$  and define the real-valued random variable  $S_Z = \text{tr}(aa^*Z)$ , where  $aa^*$  is chosen uniformly from  $\text{Cl}_n \cdot zz^*$ . Then

$$\begin{aligned} \Pr[|\text{tr}(AZ)| \geq \xi] &= \Pr[|S_Z| \geq \xi] = \Pr[S_Z^2 \geq \xi^2] \\ &\geq \Pr[S_Z^2 \geq (d+1)d\xi^2 \mathbb{E}[S_Z^2]], \end{aligned}$$

where the last inequality follows from (41), because every  $Z \in T_{\rho,r}$  obeys  $\|Z\|_2 = 1$ . Applying the Paley-Zygmund inequality, see e.g. [43, Lemma 7.16], to the non-negative random variable  $S_Z^2$  yields

$$\begin{aligned} \Pr[S_Z^2 \geq (d+1)d\xi^2 \mathbb{E}[S_Z^2]] &\geq \left( 1 - (d+1)d\xi^2 \right)^2 \frac{\mathbb{E}[S_Z^2]^2}{\mathbb{E}[S_Z^4]} \\ &\geq \frac{(1 - (d+1)d\xi^2)^2}{\frac{6}{d} \|\Xi(zz^*)\|_{\ell_4}^4 \frac{\|Z\|_1^2}{\|Z\|_2^2} + 13}, \end{aligned} \tag{44}$$

where the last line is due to (42).

According to Lemma 1, each  $Z \in T_{\rho,r}$  admits the bound

$$\begin{aligned} \frac{6}{d} \|\Xi(zz^*)\|_{\ell_4}^4 \frac{\|Z\|_1^2}{\|Z\|_2^2} + 13 &\leq 6 \left( \frac{1+\rho}{\rho} \right)^2 \frac{r}{d} \|\Xi(zz^*)\|_{\ell_4}^4 + 13 \\ &\leq \frac{24}{\rho^2} \left( \frac{r}{d} \|\Xi(zz^*)\|_{\ell_4}^4 + 1 \right) \\ &= \frac{24}{\rho^2} \sqrt{\kappa(z,r)}. \end{aligned}$$

Inserting this into (44) results in a lower bound that is valid for all  $Z \in T_{\rho,r}$  simultaneously. Thus it also applies to

$$Q_{\xi}(T_{\rho,r}; A) = \inf_{Z \in T_{\rho,r}} \Pr[|(A, Z)| \geq \xi],$$

where  $(A, Z) = \text{tr}(AZ)$  and the claim follows.  $\square$

### C. A Null Space Property for Clifford orbits

We have now assembled all necessary ingredients to prove a Null Space Property in the sense of Definition 5 for random Clifford orbit measurements.

**Theorem 5.** Set  $d = 2^n$ , and fix  $1 \leq r \leq d$ ,  $\rho \in (0, 1)$ ,  $1 \leq q \leq \infty$ . Suppose that  $\mathcal{A} : H_d \rightarrow \mathbb{R}^m$  contains

$$m \geq \frac{\tilde{C}_1}{\rho^6} \kappa(z, r) r d \log(2d) \quad (45)$$

randomly chosen elements of a Clifford orbit  $\text{Cl}_n \cdot z z^*$  with  $\|z\|_{\ell_2} = 1$ . Then, with probability at least  $1 - e^{-\frac{2\rho^4 \tilde{\gamma} m}{\kappa(z, r)}}$ ,  $\mathcal{A}$  obeys the  $r/\ell_q$ -NSP from Definition 5 with parameters

$$\rho \quad \text{and} \quad \tau = \frac{\tilde{C}_3}{\rho^2} \sqrt{\kappa(z, r) d m}^{-\frac{1}{q}}. \quad (46)$$

Here,  $C_1, \tilde{C}_3$  and  $\tilde{\gamma}$  denote constants of sufficient size.

We point out that the sampling rate (45) scales non-optimally in the NSP parameter  $\rho \in (0, 1)$ . The required sampling rate in comparable statements, such as [25, Theorem 3], only scales proportionally to  $\rho^{-2}$ . This non-optimality is due to the fact that the fourth moment bound in Lemma 2 implicitly depends on the “effective rank” of  $Z \in T_{\rho,r}$  which is proportional to  $\frac{r}{\rho^2}$  (see Lemma 1). In turn, this effective rank also features in the bound on  $Q_{\xi}(A; T_{\rho,r})$  and affects the results of Mendelson’s Small Ball Method. We believe that such a behavior is unavoidable when using Mendelson’s Small Method for Clifford orbits, and intend to address this issue in the future.

*Proof.* Applying Corollary 2 with  $\xi = \frac{1}{4\sqrt{(d+1)d}}$  and  $t = \rho^2 \sqrt{\frac{\tilde{\gamma} m}{\kappa(z, r)}}$ —where  $\tilde{\gamma}$  is a sufficiently small constant—implies

$$\begin{aligned} \inf_{Z \in T_{\rho,r}} \|\mathcal{A}(Z)\|_{\ell_q} &\geq m^{\frac{1}{q}-\frac{1}{2}} \left( \sqrt{m} \frac{Q_{\frac{1}{2\sqrt{(d+1)d}}}(T_{\rho,r}; A)}{4\sqrt{(d+1)d}} - 2W_m(T_{\rho,r}; A) - \frac{\rho^2}{4} \sqrt{\frac{\tilde{\gamma} m}{(d+1)d\kappa(z, r)}} \right) \\ &\geq \frac{m^{\frac{1}{q}-\frac{1}{2}}}{\sqrt{(d+1)d}} \left( \frac{\frac{9}{16}\rho^2 \sqrt{m}}{4 \times 24 \sqrt{\kappa(z, r)}} - \frac{2 \times 6.2098}{\rho} \sqrt{rd \log(2d)} - \frac{\rho^2}{4} \sqrt{\frac{\tilde{\gamma} m}{\kappa(z, r)}} \right) \\ &\geq \frac{\rho^2 m^{\frac{1}{q}-\frac{1}{2}}}{\sqrt{(d+1)d\kappa(z, r)}} \left( \frac{\sqrt{m}}{171} - 13 \sqrt{\frac{\kappa(z, r)^2}{\rho^6} rd \log(2d)} - \frac{\sqrt{\tilde{\gamma} m}}{4} \right) \end{aligned} \quad (47)$$

with probability at least  $1 - e^{-\frac{2\rho^4 \tilde{\gamma} m}{\kappa(z, r)}}$ . In the second line, we have inserted the bounds provided by Proposition 4 and Proposition 5, respectively. Let us now fix

$$m \geq \frac{\tilde{C}_1}{\rho^6} \kappa(z, r) r d \log(2d),$$

where  $\tilde{C}_1$  is a sufficiently large constant. Note that such a choice in particular assures  $m \geq 2d \log(d)$  which justifies the applicability of Proposition 4. Moreover, provided that  $\tilde{\gamma}$  is small enough, this choice assures that the bracket expression in (47) is lower bounded by  $\frac{2\sqrt{m}}{\tilde{C}_3}$ , where  $\tilde{C}_3$  is constant. Inserting this novel bound into

(47) allows us to conclude

$$\inf_{Z \in T_{\rho,r}} \|\mathcal{A}(Z)\|_{\ell_q} \geq \frac{2\rho^2 m^{\frac{1}{q}}}{\tilde{C}_3 \sqrt{(d+1)d\kappa(z, r)}} \geq \frac{\rho^2 m^{\frac{1}{q}}}{\tilde{C}_3 d \sqrt{\kappa(z, r)}}$$

with high probability. Inserting this bound into (35) establishes the claimed Null Space Property for  $\mathcal{A}$  with probability at least  $1 - e^{-\frac{2\rho^4 \tilde{\gamma} m}{\kappa(z, r)}}$ .  $\square$

### D. Derivation of Theorem 1

Suppose that  $\mathcal{A} : H_d \rightarrow \mathbb{R}^m$  obeys a  $r/\ell_q$ -NSP in the sense of Definition 5. Then, every approximately rank- $r$  matrix  $X \in H_d$  can be estimated from noisy measurements of the form  $y = \mathcal{A}(X) + \epsilon$ . One way to achieve stable reconstruction is via constrained nuclear norm minimization (15), provided that the parameter  $\eta$  obeys  $\eta \geq \|\epsilon\|_{\ell_q}$ :

**Theorem 6** (Theorem 3.3 in [25] for hermitian matrices). *Fix  $r, q \geq 1$  and suppose that  $\mathcal{A} : H_d \rightarrow \mathbb{R}^m$  obeys a  $r/\ell_q$ -NSP with constants  $\rho \in (0, 1)$  and  $\tau > 0$ . Then*

$$\|Z - X\|_2 \leq \frac{C_\rho}{\sqrt{r}}(\|Z\|_1 - \|X\|_1 + 2\sigma_r(X)) + D_\rho \tau \|\mathcal{A}(Z - X)\|_{\ell_q} \quad \forall X, Z \in H_d, \quad (48)$$

with  $C_\rho = \frac{(1+\rho)^2}{1-\rho}$  and  $D_\rho = \frac{3+\rho}{1-\rho}$ .

Now let  $X \in H_d$  be the matrix of interest and  $Z^\sharp$  be the minimizer of (15). By construction,  $X$  is also a feasible point of this minimization and optimality of  $Z^\sharp$  assures  $\|Z^\sharp\|_1 - \|X\|_1 \leq 0$ . Moreover:

$$\begin{aligned} \|\mathcal{A}(X) - Z\|_{\ell_q} &\leq \|\mathcal{A}(X) - y\|_{\ell_q} + \|\mathcal{A}(Z) - y\|_{\ell_q} \\ &\leq \|\epsilon\|_{\ell_q} + \eta \leq 2\eta. \end{aligned}$$

Inserting these inequalities into (48) implies

$$\|Z^\sharp - X\|_2 \leq \frac{2C_\rho}{\sqrt{r}}\sigma_r(X)_1 + 2D_\rho\tau\eta, \quad (49)$$

provided that  $\mathcal{A}$  obeys a  $r/\ell_q$ -NSP.

Now, set  $d = 2^n$  and fix  $\rho = \rho_0 \in (0, 1)$ , as well as

$$C_1 \geq \frac{2\tilde{C}_1}{\rho_0^6} \quad \text{and} \quad \gamma = 2\rho_0^4\tilde{\gamma},$$

where  $\tilde{C}_1, \tilde{\gamma}_1$  are constants featuring in Theorem 5. This statement then assures that choosing

$$m \geq C_1\kappa(z, r)rd \log(d) \geq \frac{\tilde{C}_1}{\rho_0^6}\kappa(z, r)rd \log(2d)$$

random elements of a Clifford orbit  $\text{Cl}_n \cdot zz^*$  results in a measurement operator  $\mathcal{A} : H_d \rightarrow \mathbb{R}^m$  that obeys a  $r/\ell_q$ -NSP with probability at least  $1 - e^{-\frac{\gamma m}{\kappa(z, r)}}$ . The associated constants are

$$\rho = \rho_0 \quad \text{and} \quad \tau = \frac{\tilde{C}_3}{\rho_0^2} \sqrt{\kappa(z, r)} dm^{-\frac{1}{q}}.$$

Inserting these constants into (49) then implies

$$\|Z^\sharp - X\|_2 \leq \frac{C_2}{\sqrt{r}}\sigma_r(X) + C_3 \sqrt{\kappa(z, r)} dm^{-\frac{1}{q}} \eta$$

with constants  $C_2 = \frac{2(1+\rho_0)^2}{1-\rho_0}$  and  $C_3 = \tilde{C}_3 \frac{(3+\rho_0)}{(1-\rho_0)\rho_0^2}$ .

### E. Extension to positive semidefinite matrix reconstruction

Suppose that the matrices of interest  $X \in H_d$  are not only approximately low rank, but also positive semidefinite. Also, we shall assume a phaseless measurement process  $A_k = a_k a_k^*$  that is isotropic in the sense that

$$\mathbb{E}[A_k] = \frac{1}{d}\mathbb{I}.$$

Note that this is the case for random Clifford orbit measurements, since they obey equation (27) for  $t = 1$ . For any  $\beta \in (0, 1)$  this expected concentration together with unit normalization of the  $a_k$ 's implies that the measurement matrices contained in a concrete sampling operator  $\mathcal{A} : H_d \rightarrow \mathbb{R}^m$  obey

$$\Pr \left[ \left\| \frac{d}{m} \sum_{k=1}^m a_k a_k^* - \mathbb{I} \right\|_\infty \geq \beta \right] \leq d e^{-\frac{4\beta^2 m}{8(d+1)}}. \quad (50)$$

This follows from standard matrix concentration inequalities, see for instance [25, Proof of Proposition 8.2]. We shall fix  $Y_{\mathcal{A}} := \frac{d}{m} \sum_{k=1}^m a_k a_k^* \in H_d$  and  $\beta_0 = \frac{\sqrt{2}-1}{\sqrt{2}+1}$  which both may not be optimal—to simplify presentation in the remainder of this section.

Positive semi-definiteness of  $X$  and  $\|Y_{\mathcal{A}} - \mathbb{I}\|_\infty \leq \beta$  allows for replacing constrained nuclear norm minimization (15) by the simpler reconstruction algorithm (17):

$$Z^\sharp = \underset{Z \geq 0}{\operatorname{argmin}} \|\mathcal{A}(Z) - y\|_{\ell_q}.$$

**Theorem 7** (Special case of Theorem 8.1 in [25]). *Fix  $r, q \geq 1$  and suppose that  $\mathcal{A} : H_d \rightarrow \mathbb{R}^m$  obeys a  $r/\ell_q$ -NSP with parameters  $\rho \in (0, \frac{1}{2})$  and  $\tau > 0$ , as well as  $\|Y_{\mathcal{A}} - \mathbb{I}\|_\infty \leq \beta_0$ . Then, any pair  $X, Z \in H_d$  of positive semidefinite matrices obeys*

$$\|Z - X\|_2 \leq \frac{\bar{C}_\rho}{\sqrt{r}}\sigma_r(X) + \bar{D}_\rho \left( dm^{-\frac{1}{q}} + \tau \right) \|\mathcal{A}(X - Z)\|_{\ell_q}$$

with  $\bar{C}_\rho = 4 \frac{(1+2\rho)^2}{1-2\rho}$  and  $\bar{D}_\rho = 2 \frac{3+2\rho}{1-2\rho}$ .

Now note that the minimizer  $Z^\sharp$  of (17), as well as any matrix  $X$  of interest are positive semidefinite. Moreover,  $Z^\sharp$  obeys

$$\begin{aligned} \|\mathcal{A}(X - Z^\sharp)\|_{\ell_q} &= \|y - \epsilon - \mathcal{A}(Z^\sharp)\|_{\ell_q} \\ &\leq \|\epsilon\|_{\ell_q} + \|\mathcal{A}(Z^\sharp) - y\|_{\ell_q} \\ &\leq \|\epsilon\|_{\ell_q} + \|\mathcal{A}(X) - y\|_{\ell_q} = 2\|\epsilon\|_{\ell_q}, \end{aligned}$$

where the last inequality is due to the fact that  $X$  itself is a feasible point of the optimization (17). Inserting this bound into the assertion of Theorem 7 gives

$$\|Z^\sharp - X\|_2 \leq \frac{\bar{C}_\rho}{\sqrt{r}}\sigma_r(X) + 2\bar{D}_\rho (dm^{-\frac{1}{q}} + \tau) \|\epsilon\|_{\ell_q}. \quad (51)$$

In order to derive Theorem 2, we fix  $d = 2^n$ ,  $\rho = \rho_0 \in (0, \frac{1}{2})$  and once more set  $C_1 \geq \frac{2\tilde{C}_1}{\rho_0^2}$  and  $\gamma = 2\rho_0^4\tilde{\gamma}$ . Then for any  $r, q$ , Theorem 5 assures that a measurement operator  $\mathcal{A} : H_d \rightarrow \mathbb{R}^m$  containing  $m \geq C_1\kappa(z, r)rd \log(d)$  random elements of a Clifford orbit  $\text{Cl}_n \cdot \text{ZZ}^*$  obeys the  $r/\ell_q$ -NSP with parameters  $\rho = \rho_0$  and  $\tau = \frac{\tilde{C}_3}{\rho_0^2} \sqrt{\kappa(z, r)} dm^{-\frac{1}{q}}$ . The probability of failure for this to be true is bounded by  $e^{-\frac{\gamma m}{\kappa(z, r)}}$ .

Moreover, Eq. (50) asserts that the second condition in Theorem 7, namely  $\|\mathcal{Y}_{\mathcal{A}} - \mathbb{I}\|_{\infty} \leq \beta_0$ , is met with probability at least  $1 - de^{-\frac{\beta_0^2 m}{8(d+1)}}$ .

A union bound over these two individual probabilities of failure yields

$$e^{-\frac{\gamma m}{\kappa(z, r)}} + de^{-\frac{4\beta_0^2 m}{8(d+1)}} \leq (d+1)e^{-\frac{\min\{\frac{1}{2}\beta_0^2, \gamma\} m}{\max\{\kappa(z, r), 8(d+1)\}}} \leq (d+1)e^{-\frac{\gamma m}{d+1}}$$

Provided that both assertions hold true, Eq. (51) implies

$$\begin{aligned} \|Z^{\#} - X\|_2 &\leq \frac{\tilde{C}_{\rho_0}}{\sqrt{r}} \sigma_r(X) + 2\tilde{D}_{\rho_0} \left( dm^{-\frac{1}{q}} + \tau \right) \|\epsilon\|_{\ell_q} \\ &\leq \frac{\hat{C}_2}{\sqrt{r}} \sigma_r(X) + \hat{C}_3 \sqrt{\kappa(z, r)} dm^{-\frac{1}{q}} \|\epsilon\|_{\ell_q} \end{aligned}$$

with constants  $\hat{C}_2 = \frac{(1+2\rho)^2}{1-2\rho}$  and  $\hat{C}_3 = 4\frac{3+2\rho}{1-2\rho} \left(1 + \frac{\tilde{C}_3}{\rho_0^2}\right)$ .

### Acknowledgments

This work has been supported by the Excellence Initiative of the German Federal and State Governments (Grant ZUK 81), the ARO under contract W911NF-14-1-0098 (Quantum Characterization, Verification, and Validation), and the DFG (SPP1798 CoSIP). Major parts of this project were undertaken while DG and RK participated in the *Mathematics of Signal Processing* program of the Hausdorff Research Institute of Mathematics at the University of Bonn.

### VII. APPENDIX: RECONSTRUCTING STABILIZER STATES FROM STABILIZER MEASUREMENTS

Here, we present a heuristic argument that suggests that  $O(n^2)$  noise-free stabilizer measurements might be sufficient to identify an unknown stabilizer state. The argument neither suggests an algorithm, nor does it seem easy to base a rigorous proof on it.

We note that there are results (e.g. the presentation archived at [87] and an announcement [88] of results due to Montanaro, Aaronson, Chen, Gottesman, and

Liew) in quantum information stating that a stabilizer state can be identified from  $O(n)$  measurements of stabilizer bases. These results come with matching converses, based on Holevo's bound. Their  $O(n)$  basis measurements involve  $O(n)2^n$  inner products – exponentially more than we conjecture are necessary. There is no direct contradiction, however, as the quantum model is weaker than the one employed here: In the quantum setup, the squared inner products  $|\langle a_k, x \rangle|^2$  need to be estimated through quantum mechanical experiments, while in the classical noise-free model, we have direct access to their values.

For the analysis, we assume that  $x, a_1, \dots, a_m$  are uniformly drawn stabilizer states and set  $y_k = |\langle x, a_k \rangle|^2$ . Recovery is possible when

$$I(x : y_1, \dots, y_m | a_1, \dots, a_m) = H(x),$$

i.e. when the mutual information between the object  $x$  to be recovered and the outcomes  $y_k$ , conditioned on the choices of measurement, reach the entropy of  $x$ . Here, we compute  $H(x)$  and

$$I(x : y_k | a_k) = H(y_k | a_k).$$

using the results of Ref. [37].

Adopting the notation of Ref. [37], the entropy of  $x$  is

$$H(x) = \log_2 |\text{Stabs}(2, n)| \simeq \frac{1}{2}n(n+1) = \mathcal{O}(n^2).$$

The approximation becomes tight as  $n \rightarrow \infty$ , as can be checked numerically using the explicit formulas in [37, 89].

To compute  $H(y_k | a_k)$ , we need to find the distribution of  $y_k$ , i.e. of the squared inner product between a fixed stabilizer state  $a_k$  and a random one  $x$ . Let  $K$  be the intersection between the Lagrangian subspaces associated with  $a_k$  and with  $x$ , respectively. Then according to [37], the squared inner product  $y_k$  is equal to  $2^{\dim K - n}$  if the respective phase functions agree on  $K$ ; else it is equal to 0. The former event occurs with probability  $2^{-\dim K}$ . Based on this, one can compute the distribution of  $y_k$  conditioned on  $a_k$ :

$$\begin{aligned} \Pr[y_k = 0 | a_k] &= \sum_{l=0}^n (1 - 2^{-l}), \\ \Pr[y_k = 2^{-l} | a_k] &= 2^{-l} \frac{\kappa(2, n, l)}{|\text{Stabs}(2, n)|} \quad (l = 0, \dots, n), \end{aligned}$$

where, following [37],  $\kappa(2, n, l)$  denotes the number of Lagrangian subspaces intersecting a given Lagrangian subspace in  $l$  dimensions. One can plug these expressions into a computer algebra system to compute the entropy of the distribution. It turns out to converge as  $n \rightarrow \infty$  to

$$I(x : y_k | a_k) = H(y_k | a_k) \simeq 1.719 = \mathcal{O}(1).$$

Now it is *not* true that  $I(x : y_1, \dots, y_m | a_1, \dots, a_m)$  equals  $m I(x : y_k | a_k)$ . But it seems to us to be a plausible



assumption that the conditional mutual information increases roughly linearly with  $m$  until it reaches  $H(x)$ . If true, this would imply that recovery is possible from

$$m \simeq H(x)/I(x : y_k | a_k) = \mathcal{O}(n^2)$$

stabilizer measurements.

Verifying or disproving this statement is an interesting open problem.

- 
- [1] A. Walther, "The question of phase retrieval in optics," *J. Mod. Optic.*, vol. 10, no. 1, pp. 41–49, 1963.
  - [2] R. Millane, "Phase retrieval in crystallography and optics," *JOSA A*, vol. 7, pp. 394–411, 1990.
  - [3] C. Fienup and J. Dainty, "Phase retrieval and image reconstruction for astronomy," in *Image Recovery: Theory and Application*, pp. 231–275, Elsevier, 1987.
  - [4] J. R. Fienup, J. C. Marron, T. J. Schulz, and J. H. Seldin, "Hubble space telescope characterized by using phase-retrieval algorithms," *Appl. Optics*, vol. 32, no. 10, pp. 1747–1767, 1993.
  - [5] H. N. Chapman, A. Barty, M. J. Bogan, S. Boutet, M. Frank, S. P. Hau-Riege, S. Marchesini, B. W. Woods, S. Bajt, W. H. Benner, *et al.*, "Femtosecond diffractive imaging with a soft-X-ray free-electron laser," *Nat. Phys.*, vol. 2, no. 12, pp. 839–843, 2006.
  - [6] F. Pfeiffer, T. Weitkamp, O. Bunk, and C. David, "Phase retrieval and differential phase-contrast imaging with low-brilliance X-ray sources," *Nat. Phys.*, vol. 2, no. 4, pp. 258–261, 2006.
  - [7] S. T. Flammia, A. Silberfarb, and C. M. Caves, "Minimal informationally complete measurements for pure states," *Found. Phys.*, vol. 35, no. 12, pp. 1985–2006, 2005.
  - [8] A. Peres, *Quantum theory: concepts and methods*, vol. 57. Springer, 2006.
  - [9] T. Heinosaari, L. Mazzarella, and M. M. Wolf, "Quantum tomography under prior information," *Commun. Math. Phys.*, vol. 318, no. 2, pp. 355–374, 2013.
  - [10] C. H. Baldwin, I. H. Deutsch, and A. Kalev, "Strictly-complete measurements for bounded-rank quantum-state tomography," *Phys. Rev. A*, vol. 93, no. 5, p. 052105, 2016.
  - [11] C. Carmeli, T. Heinosaari, M. Kech, J. Schultz, and A. Toigo, "Efficient pure state quantum tomography from five orthonormal bases," *preprint arXiv:1604.02970*, 2016.
  - [12] J. R. Fienup, "Phase retrieval algorithms: a comparison," *Appl. Optics*, vol. 21, no. 15, pp. 2758–2769, 1982.
  - [13] E. J. Candès, Y. C. Eldar, T. Strohmer, and V. Voroninski, "Phase retrieval via matrix completion," *SIAM J. Imaging Sci.*, vol. 6, pp. 199–225, 2013.
  - [14] E. Candès, T. Strohmer, and V. Voroninski, "PhaseLift: Exact and stable signal recovery from magnitude measurements via convex programming," *Comm. Pure Appl. Math.*, vol. 66, pp. 1241–1274, 2013.
  - [15] E. J. Candès and X. Li, "Solving quadratic equations via PhaseLift when there are about as many equations as unknowns," *Found. Comput. Math.*, pp. 1–10, 2013.
  - [16] D. Gross, F. Krahmer, and R. Kueng, "A partial derandomization of PhaseLift using spherical designs," *J. Fourier Anal. Appl.*, pp. 1–38, 2014.
  - [17] B. Alexeev, A. S. Bandeira, M. Fickus, and D. G. Mixon, "Phase retrieval with polarization," *SIAM J. Imaging Sci.*, vol. 7, no. 1, pp. 35–66, 2014.
  - [18] E. J. Candès, X. Li, and M. Soltanolkotabi, "Phase retrieval from coded diffraction patterns," *Appl. Comput. Harmonic Anal.*, vol. 39, no. 2, pp. 277–299, 2015.
  - [19] D. Gross, F. Krahmer, and R. Kueng, "Improved recovery guarantees for phase retrieval from coded diffraction patterns," *Appl. Comput. Harmonic Anal.*, 2015. doi:10.1016/j.acha.2015.05.004.
  - [20] R. Kueng, "Low rank matrix recovery from few orthonormal basis measurements," in *2015 International Conference on Sampling Theory and Applications (SampTA)*, pp. 402–406, IEEE, 2015.
  - [21] R. Kueng, H. Rauhut, and U. Terstiege, "Low rank matrix recovery from rank one measurements," *Appl. Comput. Harmonic Anal.*, 2015. DOI:10.1016/j.acha.2015.07.007.
  - [22] P. Salanevich and G. E. Pfander, "Polarization based phase retrieval for time-frequency structured measurements," in *2015 International Conference on Sampling Theory and Applications (SampTA)*, pp. 187–191, IEEE, 2015.
  - [23] J. A. Tropp, "Convex recovery of a structured signal from independent random linear measurements," in *Sampling Theory, a Renaissance*, pp. 67–101, Birkhäuser/Springer, 2015.
  - [24] F. Krahmer and Y.-K. Liu, "Phase retrieval without small-ball probability assumptions," *preprint arXiv:1604.07281*, 2016.
  - [25] M. Kabanava, R. Kueng, H. Rauhut, and U. Terstiege, "Stable low-rank matrix recovery via null space properties," *Inf. Inference*, 2016. doi:10.1093/imaiai/iaw014.
  - [26] M. Kech, "Explicit frames for deterministic phase retrieval via phaselift," *preprint arXiv:1508.00522*, 2015.
  - [27] B. G. Bodmann and N. Hammen, "Algorithms and error bounds for noisy phase retrieval with low-redundancy frames," *Appl. Comput. Harmonic Anal.*, 2016.
  - [28] V. Pohl, F. Yang, and H. Boche, "Phaseless signal recovery in infinite dimensional spaces using structured modulations," *J. Fourier Anal. Appl.*, vol. 20, no. 6, pp. 1212–1233, 2014.
  - [29] P. Delsarte, J.-M. Goethals, and J. J. Seidel, "Spherical codes and designs," *Geometriae Dedicata*, vol. 6, no. 3, pp. 363–388, 1977.
  - [30] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, "Symmetric informationally complete quantum measurements," *J. Math. Phys.*, vol. 45, no. 6, pp. 2171–2180, 2004.
  - [31] R. Kueng, D. Gross, and F. Krahmer, "Spherical designs as a tool for derandomization: The case of PhaseLift," in *2015 International Conference on Sampling Theory and Applications (SampTA)*, pp. 192–196, May 2015.
  - [32] M. Ehler, M. Gräf, and F. J. Király, "Phase retrieval using random cubatures and fusion frames of positive semidefinite matrices," *Waves, Wavelets and Fractals*, vol. 1, no. 1, 2015.
  - [33] A. Ambainis and J. Emerson, "Quantum  $t$ -designs:  $t$ -wise independence in the quantum world," in *22nd Annual IEEE Conference on Computational Complexity (CCC'07)*,

- pp. 129–140, June 2007.
- [34] F. G. Brandao, A. W. Harrow, and M. Horodecki, “Local random quantum circuits are approximate polynomial-designs,” *preprint arXiv:1208.0692*, 2012.
  - [35] H. Zhu, “Multiqubit Clifford groups are unitary 3-designs,” *preprint arXiv:1510.02619*, 2015.
  - [36] Z. Webb, “The Clifford group forms a unitary 3-design,” *preprint arXiv:1510.02769*, 2015.
  - [37] R. Kueng and D. Gross, “Qubit stabilizer states are complex projective 3-designs,” *preprint arXiv:1510.02767*, 2015.
  - [38] A. Klappenecker and M. Rotteler, “Mutually unbiased bases are complex projective 2-designs,” in *2005 IEEE International Symposium on Information Theory (ISIT), Vols 1 and 2*, pp. 1740–1744, 2005.
  - [39] B. G. Bodmann and J. Haas, “Achieving the orthoplex bound and constructing weighted complex projective 2-designs with Singer sets,” *preprint arXiv:1509.05333*, 2015.
  - [40] R. Kueng, H. Zhu, M. Grassl, and D. Gross, “Distinguishing quantum states using Clifford orbits,” *preprint arXiv:1609.08595*, 2016.
  - [41] J. Perina, Z. Hradil, and B. Jurco, *Quantum optics and fundamentals of physics*. Springer, 2012.
  - [42] K. Banaszek, M. Cramer, and D. Gross, “Focus on quantum tomography,” *New J. Phys.*, vol. 15, no. 12, p. 125020, 2013.
  - [43] S. Foucart and H. Rauhut, *A Mathematical Introduction to Compressive Sensing*. Applied and Numerical Harmonic Analysis, Birkhäuser/Springer, New York, 2013.
  - [44] D. L. Donoho, “Compressed sensing,” *IEEE Trans. Inform. Theory*, vol. 52, no. 4, pp. 1289–1306, 2006.
  - [45] E. J. Candès and T. Tao, “Near-optimal signal recovery from random projections: Universal encoding strategies?,” *IEEE Trans. Inform. Theory*, vol. 52, no. 12, pp. 5406–5425, 2006.
  - [46] E. J. Candès, J. K. Romberg, and T. Tao, “Stable signal recovery from incomplete and inaccurate measurements,” *Commun. Pur. Appl. Math.*, vol. 59, no. 8, pp. 1207–1223, 2006.
  - [47] E. J. Candès, J. Romberg, and T. Tao, “Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information,” *IEEE Trans. Inform. Theory*, vol. 52, no. 2, pp. 489–509, 2006.
  - [48] T. Tao, “An uncertainty principle for cyclic groups of prime order,” *preprint math/0308286*, 2003.
  - [49] B. Recht, M. Fazel, and P. A. Parrilo, “Guaranteed minimum-rank solutions of linear matrix equations via nuclear norm minimization,” *SIAM Rev.*, vol. 52, no. 3, pp. 471–501, 2010.
  - [50] E. J. Candès and B. Recht, “Exact matrix completion via convex optimization,” *Found. Comput. Math.*, vol. 9, no. 6, pp. 717–772, 2009.
  - [51] E. J. Candès and T. Tao, “The power of convex relaxation: Near-optimal matrix completion,” *IEEE Trans. Inform. Theory*, vol. 56, no. 5, pp. 2053–2080, 2010.
  - [52] R. H. Keshavan, A. Montanari, and S. Oh, “Matrix completion from a few entries,” *IEEE Trans. Inform. Theory*, vol. 56, no. 6, pp. 2980–2998, 2010.
  - [53] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert, “Quantum state tomography via compressed sensing,” *Phys. Rev. Lett.*, vol. 105, no. 15, p. 150401, 2010.
  - [54] D. Gross, “Recovering low-rank matrices from few coefficients in any basis,” *IEEE Trans. Inform. Theory*, vol. 57, pp. 1548–1566, 2011.
  - [55] Y. K. Liu, “Universal low-rank matrix recovery from pauli measurements,” in *Advances in Neural Information Processing Systems 24*, pp. 1638–1646, Curran Associates, Inc., 2011.
  - [56] S. T. Flammia, D. Gross, Y.-K. Liu, and J. Eisert, “Quantum tomography via compressed sensing: error bounds, sample complexity and efficient estimators,” *New J. Phys.*, vol. 14, no. 9, p. 095022, 2012.
  - [57] D. Gottesman, *Stabilizer codes and quantum error correction*. PhD thesis, California Institute of Technology, Pasadena, CA, 1997.
  - [58] F. MacWilliams and N. Sloane, *The Theory of Error-correcting Codes*. North-Holland mathematical library, North-Holland Publishing Company, 1977.
  - [59] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-dual codes and invariant theory*, vol. 17. Springer, 2006.
  - [60] K. Gröchenig, *Foundations of Time-Frequency Analysis*. Applied and Numerical Harmonic Analysis, Birkhäuser Boston, 2013.
  - [61] G. Pfander, “Gabor frames in finite dimensions,” in *Finite Frames* (P. G. Casazza and G. Kutyniok, eds.), Applied and Numerical Harmonic Analysis, pp. 193–239, 2013.
  - [62] J. v. Neumann, “Die Eindeutigkeit der Schrödingerschen Operatoren,” *Math. Ann.*, vol. 104, no. 1, pp. 570–578, 1931.
  - [63] G. Mackey, *The Theory of Unitary Group Representations*. Chicago lectures in mathematics, University of Chicago Press, 1955.
  - [64] G. B. Folland, *Harmonic Analysis in Phase Space*, vol. 122 of *Annals of Mathematics Studies*. Princeton, NJ: Princeton University Press, 1989.
  - [65] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information 10th Anniversary Edition*. Cambridge University Press, 2010.
  - [66] D. Gross, “Hudson’s theorem for finite-dimensional quantum systems,” *J. Math. Phys.*, vol. 47, no. 12, p. 122107, 2006.
  - [67] E. Hostens, J. Dehaene, and B. De Moor, “Stabilizer states and Clifford operations for systems of arbitrary dimensions and modular arithmetic,” *Phys. Rev. A*, vol. 71, no. 4, p. 042315, 2005.
  - [68] D. Gross and M. Van den Nest, “The LU-LC conjecture, diagonal local operations and quadratic forms over  $\text{GF}(2)$ ,” *Quantum Inform. Comput.*, vol. 8, no. 3, pp. 263–281, 2008.
  - [69] H. Zhu, R. Kueng, M. Grassl, and D. Gross, “The Clifford group fails gracefully to be a unitary 4-design,” *preprint arXiv:1609.08172*, 2016.
  - [70] D. F. Walls and G. J. Milburn, *Quantum Optics*. Springer, 2nd ed., 2008.
  - [71] R. L. Hudson, “When is the Wigner quasi-probability density non-negative?,” *Rep. Math. Phys.*, vol. 6, no. 2, pp. 249–252, 1974.
  - [72] N. De Beaudrap, “A linearized stabilizer formalism for systems of finite dimension,” *preprint arXiv:1102.3354*, 2011.
  - [73] D. M. Appleby, “Symmetric informationally complete-positive operator valued measures and the extended Clifford group,” *J. Math. Phys.*, vol. 46, no. 5, p. 052107, 2005.
  - [74] J. Helsen, J. J. Wallman, and S. Wehner, “Representations of the multi-qubit Clifford group,” *preprint arXiv:1609.08188*, 2016.
  - [75] B. Runge, “Codes and Siegel modular forms,” *Discrete Math.*, vol. 148, no. 1, pp. 175 – 204, 1996.

- [76] R. Balan, B. G. Bodmann, P. G. Casazza, and D. Edidin, "Painless reconstruction from magnitudes of frame coefficients," *J. Fourier Anal. Appl.*, vol. 15, pp. 488–501, 2009.
- [77] L. Demanet and P. Hand, "Stable optimizationless recovery from phaseless linear measurements," *J. Fourier Anal. Appl.*, vol. 20, no. 1, pp. 199–221, 2014.
- [78] R. G. Shenoy and T. W. Parks, "The weyl correspondence and time-frequency analysis," *IEEE Trans. Signal Process.*, vol. 42, no. 2, pp. 318–331, 1994.
- [79] W. Kozek, "Spectral estimation in non-stationary environments," *PhD Thesis*, 1996.
- [80] V. Koltchinskii and S. Mendelson, "Bounding the smallest singular value of a random matrix without concentration," *Internat. Math. Res. Notices*, pp. 12991–13008, 2015.
- [81] S. Mendelson, "Learning without Concentration," *J. ACM*, vol. 62, no. 3, pp. 1–25, 2015.
- [82] E. Bannai and E. Bannai, "A survey on spherical designs and algebraic combinatorics on spheres," *European J. Combin.*, vol. 30, no. 6, pp. 1392–1425, 2009.
- [83] K. Mohan and M. Fazel, "Iterative reweighted least squares for matrix rank minimization," in *Proceedings of the Allerton Conference*, pp. 653–661, 2010.
- [84] B. Recht, W. Xu, and B. Hassibi, "Null space conditions and thresholds for rank minimization," *Math. Program.*, vol. Ser B, 127, pp. 175–211, 2011.
- [85] B. Recht, W. Xu, and B. Hassibi, "Necessary and sufficient conditions for success of the nuclear norm heuristic for rank minimization," in *Proc. 47th IEEE Conference on Decision and Control*, pp. 3065–3070, 2008.
- [86] M. Fornasier, H. Rauhut, and R. Ward, "Low-rank matrix recovery via iteratively reweighted least squares minimization," *SIAM J. Optim.*, vol. 21, no. 4, pp. 1614–1640, 2011.
- [87] S. Aaronson and D. Gottesman, "Identifying stabilizer states," 2006. <http://pirsa.org/08080052/>.
- [88] A. Montanaro, "Three quantum learning algoirhtms," 2013. <https://people.maths.bris.ac.uk/~csxam/presentations/learning>
- [89] S. Aaronson and D. Gottesman, "Improved simulation of stabilizer circuits," *Phys. Rev. A*, vol. 70, no. 5, p. 052328, 2004.